Neusoft

东软 NetEye 入侵检测系统 V2.2

用户使用指南

版本 1.0

2019 年 6 月

联系信息

网站：http://www.neusoft.com

电子信箱：servicedesk@neusoft.com

服务电话：400 655 6789

目录

前言

文档目标

本文档介绍如何使用东软 NetEye 入侵检测系统（以下简称“NetEye IDS ”）。

阅读对象

本文档适用于配置和管理 NetEye IDS 设备的网络管理员，同时该文档也可用于其他人员了解本设备。

文档读者需有一定的网络基础知识。

手册构成

本文档由以下几个部分组成：

- 第 1 章，系统概述概括性地介绍了系统的功能和登录方法等。
- 第 2 章，系统主页介绍登录后显示页面的各个参数。
- 第 3 章，策略管理介绍如何为系统配置策略。
- 第 4 章，实时监控介绍如何查看监控数据及监控参数的意义。
- 第 5 章，网络审计介绍记录的网络审计内容。
- 第 6 章，报表管理介绍如何创建报表计划、下载报表和阅读报表。
- 第 7 章，系统维护介绍系统自身基础功能的配置方式。
- 第 8 章，集控中心介绍如何集中管理多台设备。
- 第 9 章，日志审计介绍如何查看网络日志和系统日志。
- 第 10 章，典型部署示例举例介绍典型部署场景。

文档约定

提示：此格式中文字用于提醒读者注意某些不可忽视的事项。

第1章 系统概述

本章介绍 NetEye IDS 的概要信息，包含以下内容：

1.1.产品简介

东软 NetEye 入侵检测系统（Neusoft NetEye Intrusion Detection System，以下简称 NetEye IDS）是东软自主研发的网络入侵检测系统，主要解决网络蠕虫病毒泛滥、内部人员对网络的违规使用、网络的长期健康运行无法有效保障等问题。

NetEye IDS 的三大主要功能包括：

- 攻击检测

  利用数据流智能重组，轻松处理分片和乱序数据包。综合使用模式匹配、异常识别、统计分析、协议分析、行为分析等多种方法综合检测种类繁多的攻击与入侵行为。

- 内容恢复

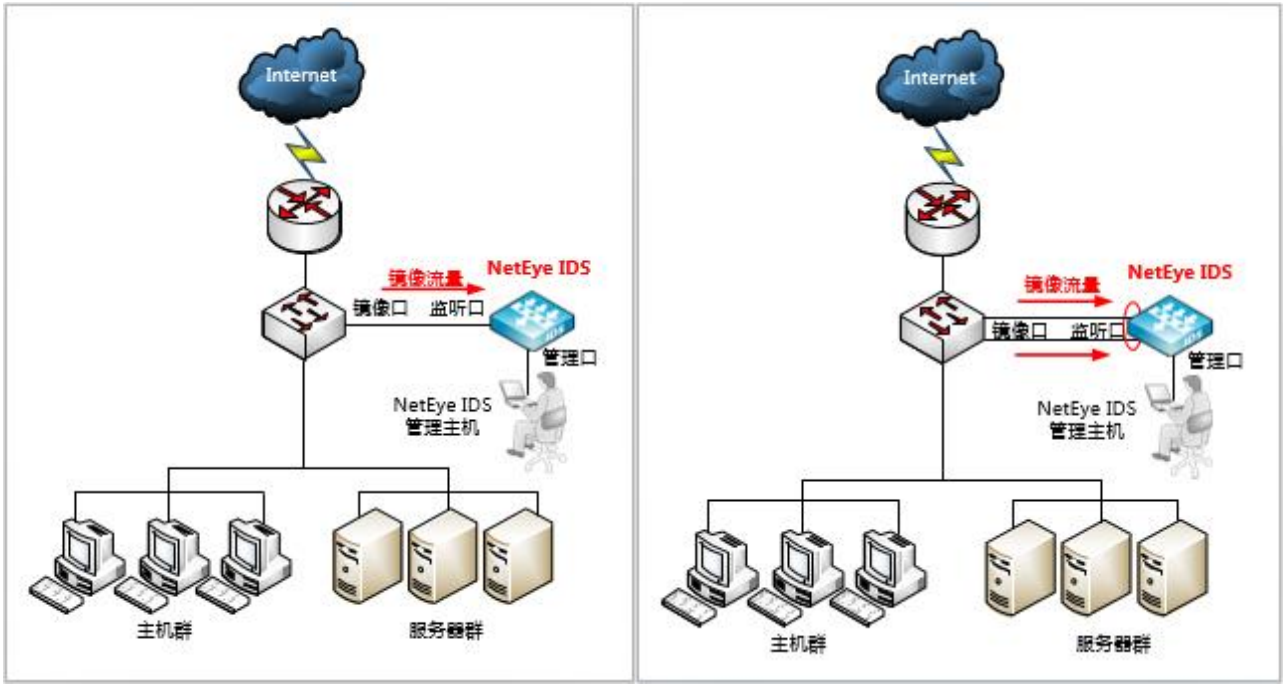
  支持对常用的应用协议的数据恢复功能，能够完全记录通信的过程与内容并将其回放。此功能对于了解攻击者的攻击过程、监控内部网络中的用户是否滥用网络资源、发现未知的攻击具有很大的作用。

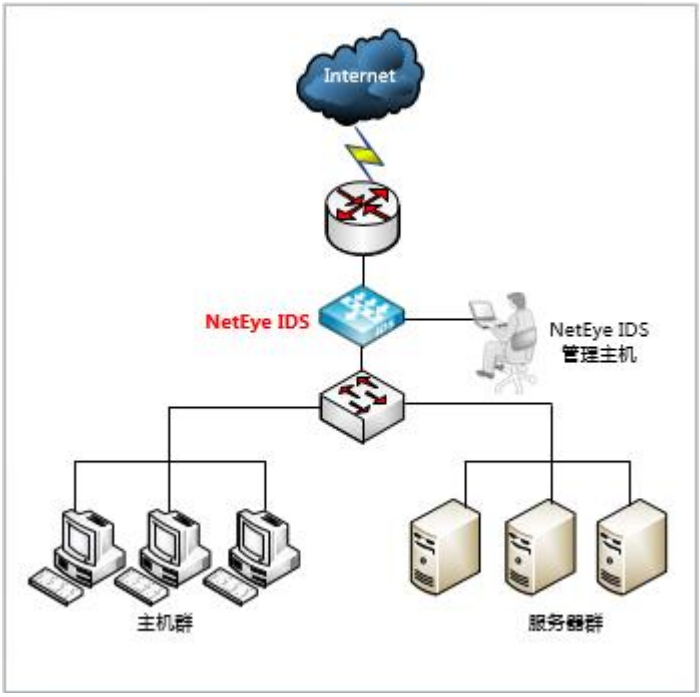
- 网络审计

  记录网络中发生的所有连接和应用，提供完整的网络审计日志。

1.2.部署方式

NetEye IDS 支持旁路和在线部署，旁路部署时一般选择使用独立监听接口接收镜像流量。如果流量超过单个接口带宽，也可以绑定监听接口以提升接收镜像流量的速度。





1.3.登录系统

NetEye IDS 出厂管理 IP 地址为 192.168.1.200/24。下面以 IE 浏览器为例，说明如何使用出厂管理地址 https://192.168.1.200 登录 NetEye IDS 的 Web 管理系统：

1. 为管理主机添加 192.168.1.0/24 网段的 IP 地址，并确认管理主机与 NetEye IDS 设备正确连接，可以互相通信。
2. 打开浏览器，输入 https://192.168.1.200。

   由于 NetEye IDS 使用的是自签名证书，这时会出现一个证书错误提示页面。点击“继续浏览此网站（不推荐）”，选择信任 NetEye IDS 的自签名证书。

3. 进入登录页面。输入缺省用户名和密码（如 root/NetEye@1996），点击**登录**，即可进入 NetEye IDS 的 Web 管理系统。

提示：缺省情况下，连续登录失败5次的用户将被禁用20分钟。

1.4.缺省管理用户

系统默认存在三个管理用户：

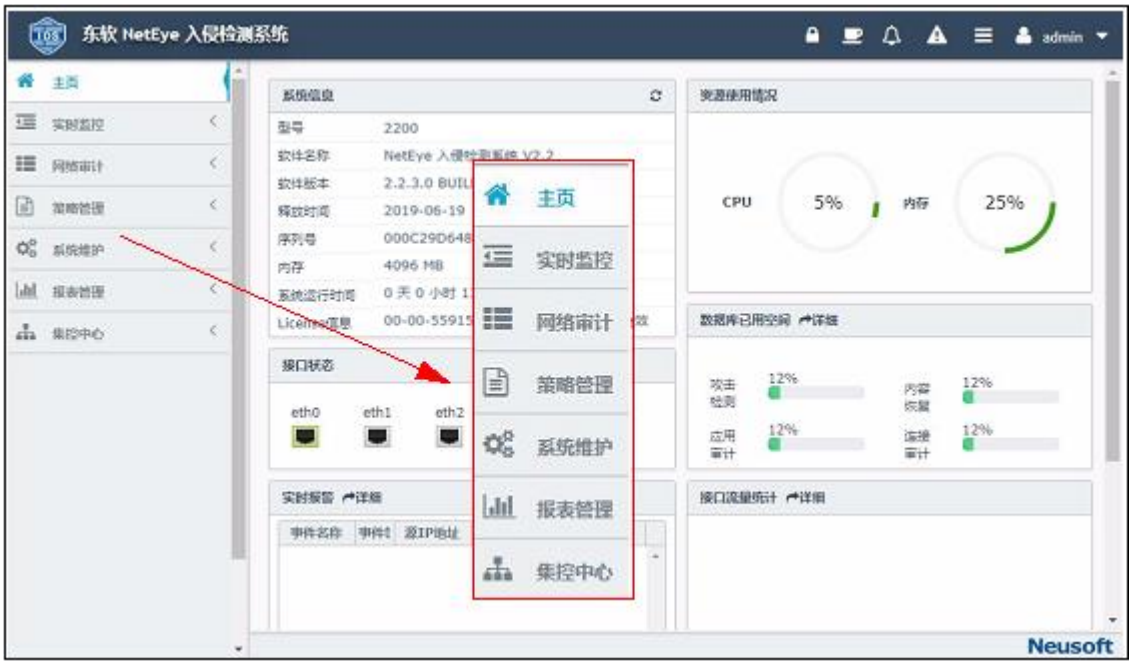
系统缺省管理用户

用户角色	缺省用户名/初始密码	权限
用户管理员	root/NetEye@1996	全局唯一，可以创建、编辑、删除安全管理员和审计员，配置密码复杂度，进行 license 管理。
安全管理员	admin/NetEye@1996	由用户管理员创建，可以实时监控系统状态和查看网络审计信息，进行策略管理、系统维护、报表管理、集中管理和策略下发。在初次登录时，需要根据提示修改初始密码。
审计员	audit/NetEye@1996	由用户管理员创建，可以进行日志审计。在初次登录时，需要根据提示修改初始密码。

用以上三种身份登录后显示如下：

- root 用户登录界面：

- admin 用户登录界面：

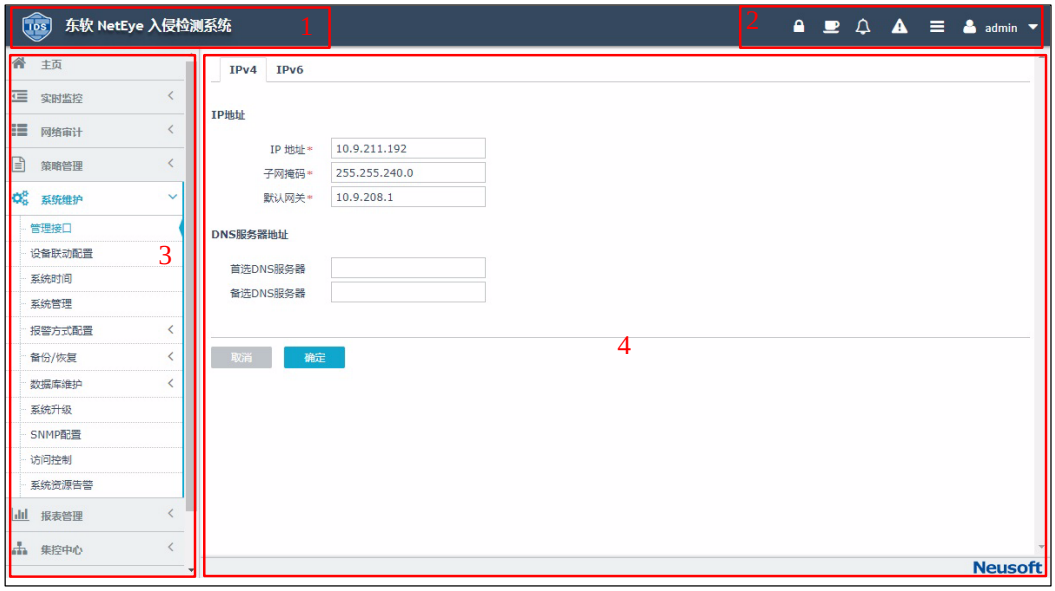


在使用 admin 账号登录时，连接流量统计栏和实时报警栏为空白。需要在安全管理员身份下，开启数据审计引擎后，方可显示全局连接流量统计。具体步骤请参见 3.1 引擎接口配置。

- audit 用户登录界面如下：

1.5.页面布局

NetEye IDS 的页面布局如下：



1. Logo 和产品名称；2. 快捷菜单；3.导航菜单；4. 查看和配置区域

NetEye IDS 提供如下快捷菜单和操作按钮：

WebUI 快捷菜单和操作按钮

快捷菜单	**描述**	**操作按钮**	**描述**
	获取资源告警状态的开关。关闭此开关将不再提示资源告警信息。		编辑条目。
	实时提示攻击检测报警状态，点击可查看详细报警信息。		删除条目。
	隐藏或显示导航菜单。		修改用户密码。
	右侧显示当前登录用户名称。		显示下拉菜单。
	点击显示更多菜单。		复制条目。
	管理员锁定 Web 管理界面。		清除内容或关闭筛选条件。
	获取配置锁。		下载文件。
	退出系统。		恢复系统数据。
	修改当前登录用户的密码。		查看条目。

第2章 系统主页

本章介绍如何查看 NetEye IDS 的主页信息。

用户管理员、安全管理员和审计员都具有查看系统主页的权限，但显示内容有所不同。用户成功登录后，将进入系统主页，可以查看如下信息：

2.1.系统信息

系统信息	
型号	2200
软件名称	NetEye 入侵检测系统 V2.2
软件版本	2.2.3.0 BUILD190619
释放时间	2019-06-19
序列号	000C29D64815
内存	4096 MB
系统运行时间	0 天 0 小时 2 分
License信息	00-00-55915-11-15-000-000-396 有效

如果未上载 License，**License 信息**后面会显示 无效 。以用户管理员身份（root）登录，点击**无效**后面的图标，可以跳转到 License 管理页面导入 License。具体操作步骤请参见 7.13 License 管理。

点击 可以刷新系统信息。

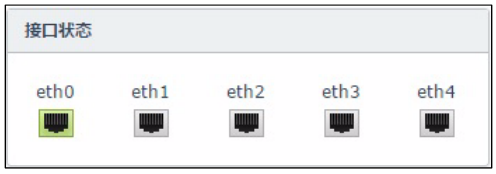
用户管理员、安全管理员、审计员全部可见。

2.2.资源使用情况

在**系统维护>系统资源告警**页面，可以设置系统资源告警阈值，及是否输出告警。

用户管理员、安全管理员、审计员全部可见。

2.3.接口状态



接口显示为灰色表示该网口没有连接网线。

用户管理员、安全管理员、审计员全部可见。

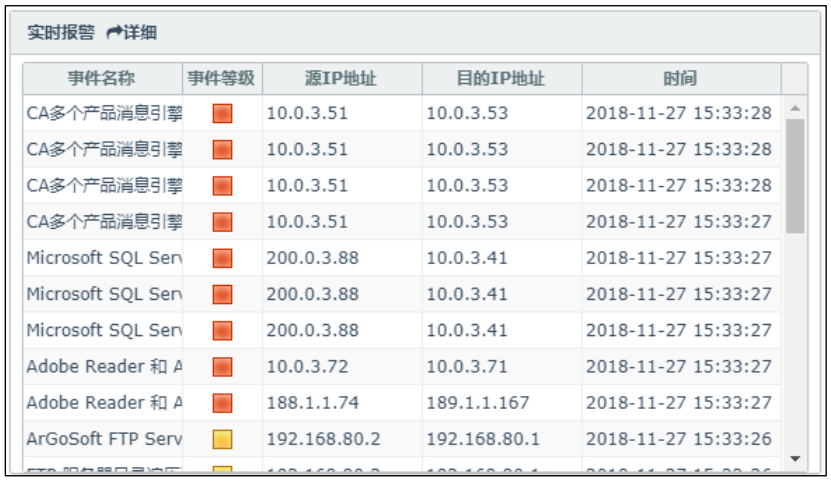
2.4.数据库已用空间

系统会自动将磁盘分配给攻击检测、内容检测、应用审计和连接审计四个功能进行使用。此处可看到四个功能模块的数据库空间使用情况。

点击**详细**链接，可跳转到**系统维护>数据库维护>数据库空间管理**页面进行各数据库清理工作。

仅安全管理员可见。

2.5.实时报警

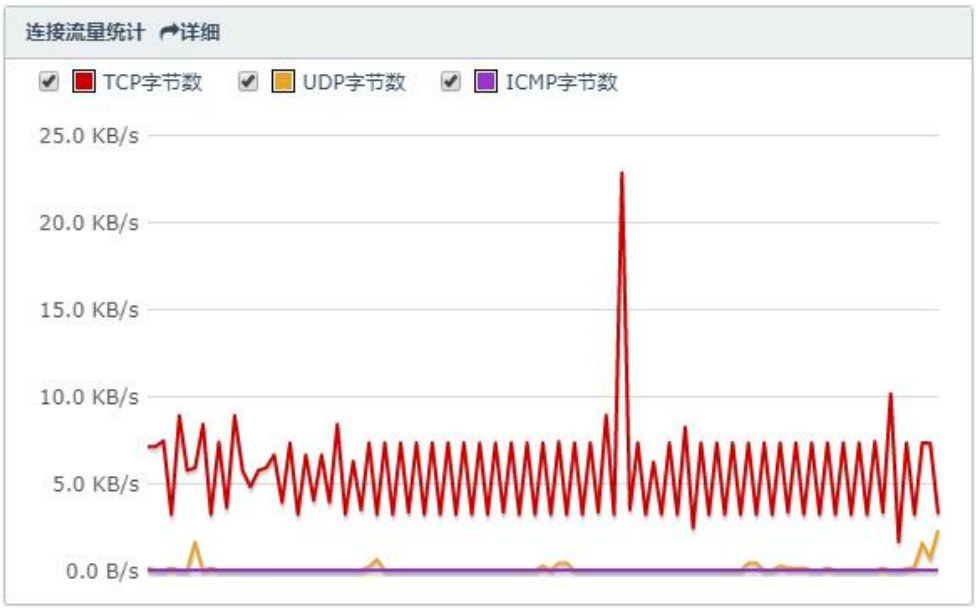


此处可查看实时报警的概要信息，包括：事件名称、事件等级、源 IP 地址、目的 IP 地址和事件发生的时间。

点击**详细**链接，可跳转到**实时监控>实时报警**页面查看报警的详细信息。

仅安全管理员可见。

2.6.连接流量统计



主页显示的是所有接口的全局流量信息，横轴表示时间，纵轴表示接口流量。接口流量的单位可随流量大小自动变化。

点击**详细**链接，可跳转到**实时监控>实时数据流量**页面查看接口详细流量信息。

仅安全管理员可见。只有在**策略管理>引擎接口配置**中打开引擎开关，并配置监听接口，此处才会显示数据。

第3章 策略管理

安全管理员可以进行策略管理，包括：

3.1.引擎接口配置

此处有数据审计引擎开关，用于开启数据审计相关功能，缺省情况下为关闭状态。如需使用实时连接状态、实时数据流量、连接审计、应用审计和内容恢复功能时，需开启此开关，并且配置监听接口。开启后，系统将实时记录上述数据以备查看。

1. 选择**策略管理>引擎接口配置**。

2. 点击**开**，开启数据审计开关。

配置完入侵检测策略后，即可配置监听接口并在监听接口上指定启用的入侵检测策略。

要配置监听接口，请以安全管理员的身份登录，并执行以下操作：

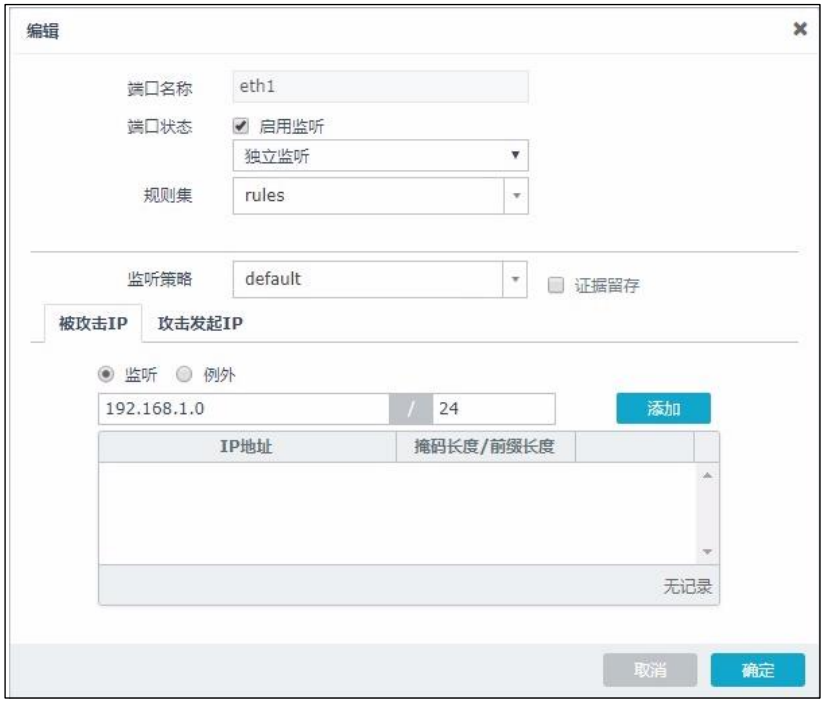
3. 选择切断模式，包括**使用接收数据包的网卡切断**和**使用 eth0 切断**。

开启切断功能后，一旦检测到触发切断的攻击，NetEye IDS 将通过所指定的网卡切断相应的 TCP 连接。

当 NetEye IDS 以旁路模式部署时，如果对端交换机的镜像接口仅允许发送流量、不允许接收流量，那么这里只能选择使用 eth0 切断连接。

提示：此处配置的切断模式只适用于在**报警配置**中开启**切断连接**功能的规则。eth0只作为管理接口，不能进行流量监听。

4. 点击接口，设置接口监听状态、监听策略和监听网络。



- **端口名称**：要启用监听功能的接口名称。
- **端口状态**：接口的监听状态和模式。启用监听功能后，需要选择监听模式：
  - **独立监听**：最常使用的工作模式，使用单一接口接收交换机发来的镜像流量。
  - **与 ethx 绑定监听**：当监听的镜像流量超过单个接口的带宽时，可以使用绑定监听，即将两个接口绑定在一起，作为一个接口接收镜像流量。此时，对端交换机的镜像接口必须是对应接口绑定形成的 Channel 接口。使用绑定监听接口时，系统默认从第二个以太网接口（eth0 除外）开始成对绑定接口，如 eth1 和 eth2、eth3 和 eth4 等。
  - **与 ethx 桥接监听**：在线部署时采用此监听模式，即从一个接口接收流量、从另外一个接口转发流量。
- **规则集**：选择在该接口上启用的跨 IP 段访问规则集，匹配到此策略的数据包将继续匹配**监听策略**。
- **监听策略**：选择在该接口上启用的入侵检测策略，默认使用 default 策略，用户可复制并修改策略。
- **证据留存**：勾选此复选框后，发生报警时，在**网络审计>攻击检测**的最后一列可以点击下载按钮，下载攻击包。
- **被攻击 IP**：选择**监听**，可以配置需要监听的可能受到攻击的 IP 地址段。选择**例外**，可以配置不进行监听的网段，其余数据则进行监听。如需监听全部流量，则不需添加任何 IP 地址段。

- **攻击发起 IP**：选择**监听**，可以配置需要监听的可能发起攻击的 IP 地址段。选择**例外**，可以配置不进行监听的网段，其余数据则进行监听。如需监听全部流量，则不需添加任何 IP 地址段。

5. 点击**确定**。

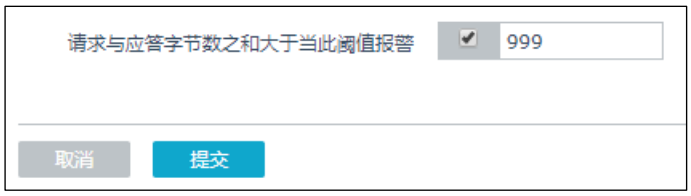
3.2.流量报警配置

本功能能够帮助管理员在流量中识别出请求与应答字节数之和大于所配阈值的连接，并在**实时监控>实时连接状态**，**网络审计>连接审计**两部分中用红色背景标识出满足条件的连接。

本功能缺省情况下为关闭状态。

要想配置此功能，请以安全管理员身份登录，并执行如下操作：

1. 选择**策略管理>流量报警配置**。
2. 勾选复选框并配置阈值大小。



3. 点击**提交**。

3.3.策略配置

配置监听接口之前，需配置入侵检测策略，指定要启用的入侵检测规则。

NetEye IDS 支持入侵检测策略和跨 IP 段访问策略。

NetEye IDS 提供一条缺省入侵检测策略 default，包含 NetEye IDS 推荐的配置，开启对一些常见的高危害攻击和威胁事件的检测。当需要根据实际情况编辑策略时，可以从配置接近的缺省策略中克隆出一个新的策略，对其进行修改。

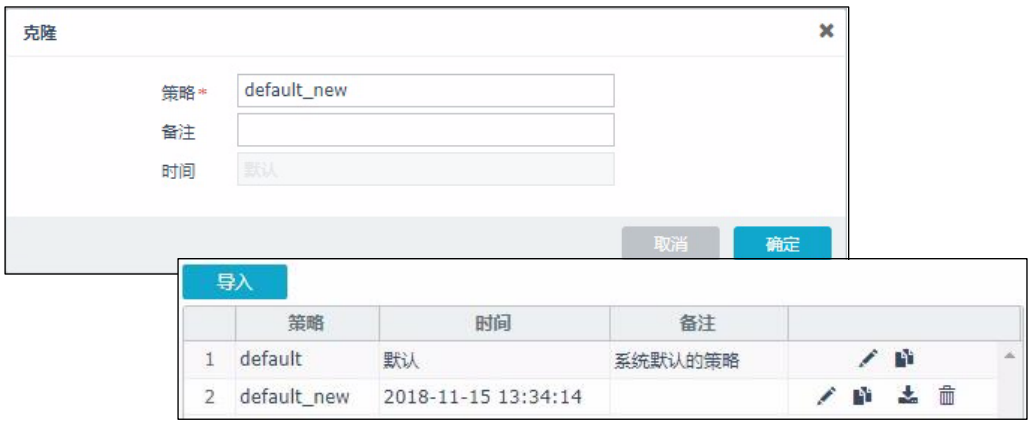
NetEye IDS 支持跨 IP 段访问策略，管理员可以通过协议、源和目的 IP 地址、源和目的端口号制定策略，并对与策略关联的事件配置等级和报警。

3.3.1. 入侵检测策略

在入侵检测策略中，管理员可以对策略进行配置，针对哪些攻击事件进行报警以及采用何种报警方式。

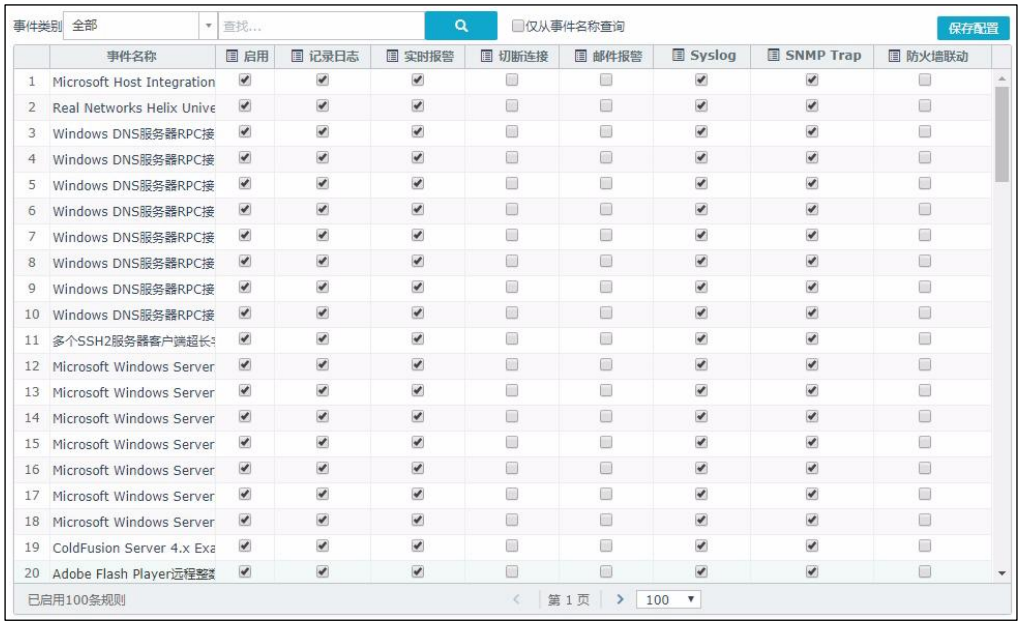
要配置入侵检测策略，请以安全管理员身份登录，并执行以下操作：

1. 选择**策略管理>策略配置>入侵检测策略**。
2. 点击 default 策略后的 ，设置克隆策略的名称和备注信息，将 default 策略克隆为一条新的策略。



点击**导入**，可导入之前更改的并导出备份的策略配置文件。

3. 点击克隆出的策略的 ，编辑策略。



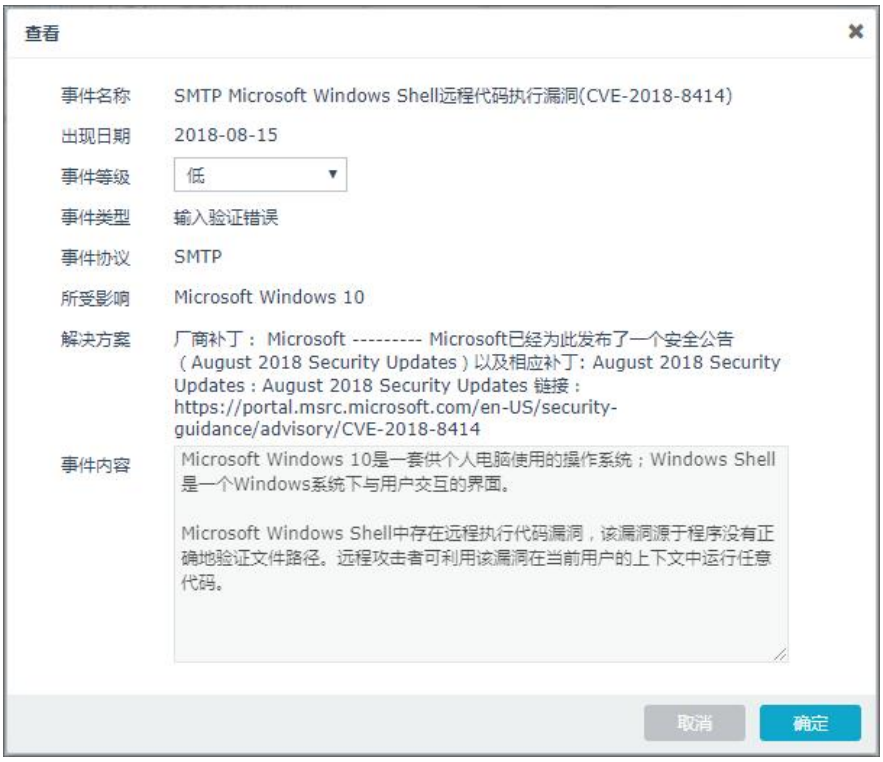
针对指定的攻击事件开启或关闭以下功能：

- **启用：是否在策略中启用针对此条事件的检测。**
- **记录日志**：检测到指定攻击事件时，是否记录日志。只有开启日志记录功能，安全管理员才可以在网络审计模块查看到攻击检测信息。
- **实时报警**：检测到指定攻击事件时，是否实时报警。开启实时报警后，检测到指定攻击事件时，界面右上角的实时报警快捷菜单将进行提示（出现红色数字，表示新出现的攻击事件数量）。
- **切断连接**：检测到指定攻击事件时，是否断开 TCP 连接。需要在设置监听接口时同时设置切断模式。关于如何设置切断模式，请参见引擎接口配置。
- **邮件报警**：检测到指定攻击事件时，是否将报警事件以邮件的形式发送给指定收件人。
- **Syslog**：检测到指定攻击事件时，是否将报警事件记录到配置的 Syslog 服务器。
- **SNMP Trap**：检测到指定攻击事件时，是否将报警事件记录到配置的 SNMP 服务器。
- **防火墙联动**：检测到指定攻击事件时，是否与防火墙联动，通过防火墙采取进一步措施。

编辑报警策略时：

- 可通过事件类型下拉菜单和查找文本框筛选要检测的攻击事件。
- 使用页面下方的下拉菜单可以选择每页显示条目数，超过选中条目数时分页显示，通过页码前后的箭头可以翻页查看。

- 使用表头项左侧的 ，可对选项进行批量选择。
- 双击条目可以查看攻击事件的详细信息，并对事件等级做修改。



4. 完成编辑后，点击右上方的**保存配置**按钮。

   如需导出修改的策略配置文件，请点击 。

   如需删除指定策略，请点击 ，并点击**确定**。

3.3.2. 跨 IP 段访问策略

3.3.2.1.事件定义

管理员可在此处配置自定义事件触发报警的名称、详细描述信息、事件等级及报警输出配置。

要配置针对特定事件的报警，请以安全管理员身份登录，并执行以下操作：

1. 选择**策略管理>跨 IP 段访问策略>事件定义**。

2. 配置自定义事件的相关信息。

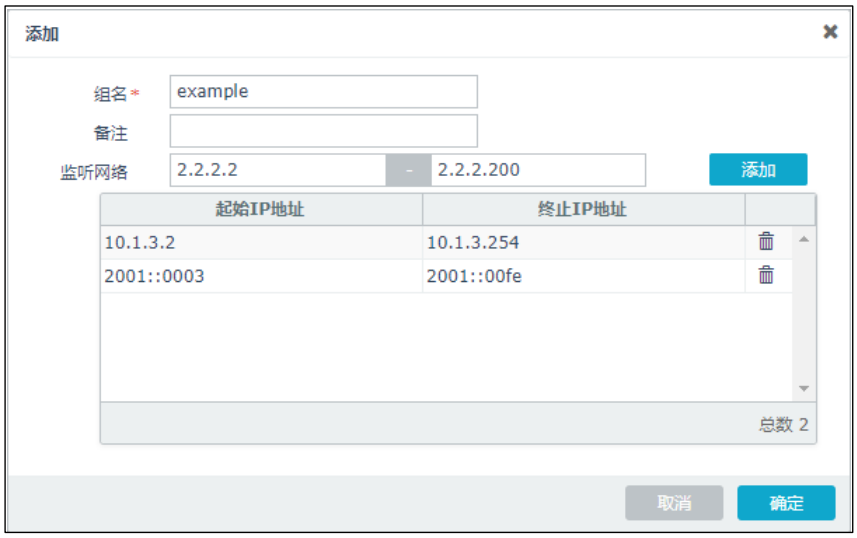
- **事件等级**：表示管理员为触发的事件指定的等级，缺省为**预警信息**。
- **报警配置**：表示输出报警的途径，缺省为**记录日志**和**实时报警**。

3.3.2.2.IP 组

管理员可在此配置 IP 地址组，供配置**规则定义**时引用。

要配置 IP 地址组，请以安全管理员身份登录，并执行以下操作：

1. 选择**策略管理>跨 IP 段访问策略> IP 组**。
2. 点击**添加**。
3. 输入需要设置的 IP 地址组，可设置多组，点击**添加**。



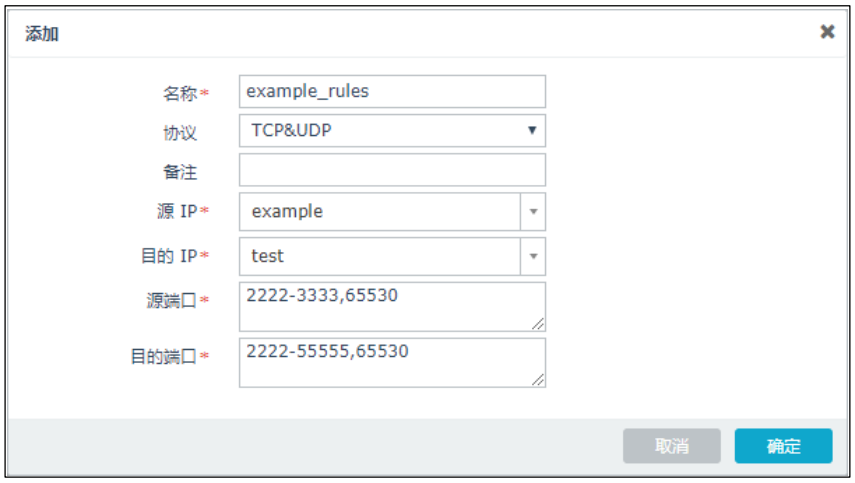
4. 点击**确定**。
5. 以相同步骤，根据需要再添加一条或多条 IP 地址组。在 3.3.2.3 白名单中，一条规则至少需要两组 IP 地址，分别为源 IP 地址组和目的 IP 地址组。

3.3.2.3.白名单

管理员可在此定义规则，供配置**报警策略**时引用。

要配置规则，请以安全管理员身份登录，并执行以下操作：

1. 选择**策略管理>跨 IP 段访问策略>白名单**。
2. 点击**添加**，填写相关信息。



- 协议：支持 IP、ICMP、TCP 和 UDP。
- 源 IP/目的 IP：选取相应的 IP 地址组。
- 源端口/目的端口：在相应的文本框中添加源端口或目的端口。多个端口号请用“,”隔开，端口号区间请输入起止端口号并用“-”连接。

3. 点击**确定**。

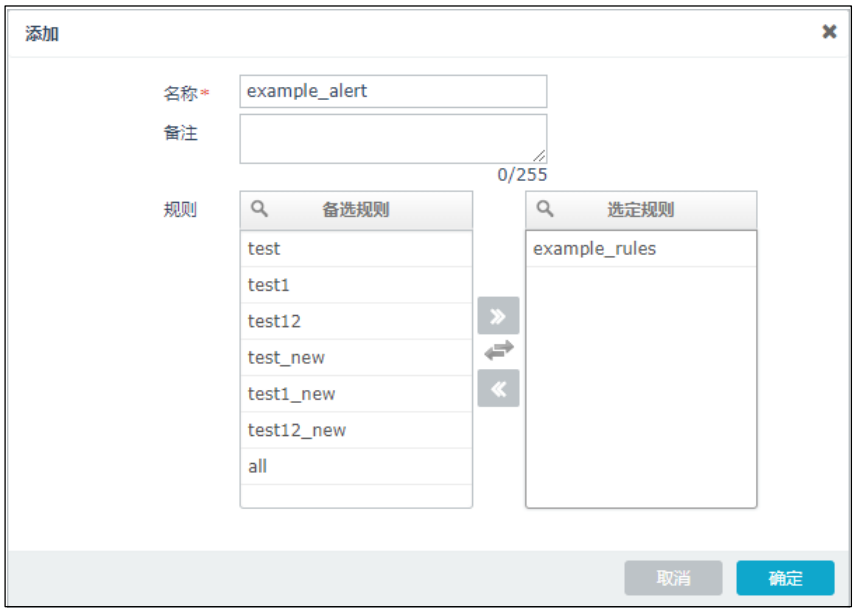
3.3.2.4.规则集

管理员可在此配置报警策略。

要配置报警策略，请以安全管理员身份登录，并执行以下操作：

1. 选择**策略管理>跨 IP 段访问策略>报警策略**。

2. 点击**添加**，输入相应信息。



3. 点击**确定**。

3.4.过滤配置

如果配置过滤功能，在系统接收到网络数据包后，会根据过滤条件来决定是否对其做进一步处理。过滤配置影响的范围包括：实时连接状态、实时数据流量、连接审计、应用审计和内容恢复。

要配置过滤功能，请以安全管理员的身份登录，并执行以下操作：

1. 选择**策略管理>过滤配置**。
2. 设置过滤协议：

3. 设置过滤端口：

端口过滤配置只针对目的端口过滤。

4. 设置过滤 IP：

5. 点击**确定**。

3.5.内容检测

NetEye IDS 可以对 HTTP、SMTP、POP3、NNTP、IMAP 等多种协议数据包的内容进行检测，并根据检测结果采取进一步的措施（标记或丢弃）。

支持的内容检测字段如下：

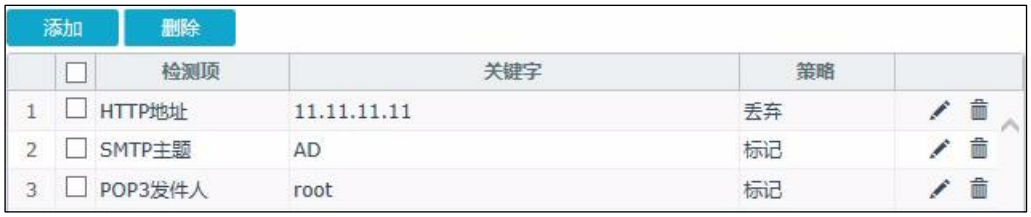
- HTTP 协议的地址和正文。
- SMTP 协议的发件人、收件人、主题和正文。
- POP3 协议的发件人、收件人、主题和正文。
- NNTP 协议的发件人、新闻组、主题和正文。
- IMAP 协议的发件人、收件人、主题和正文。

要配置内容检测，请以安全管理员的身份登录，并执行以下操作：

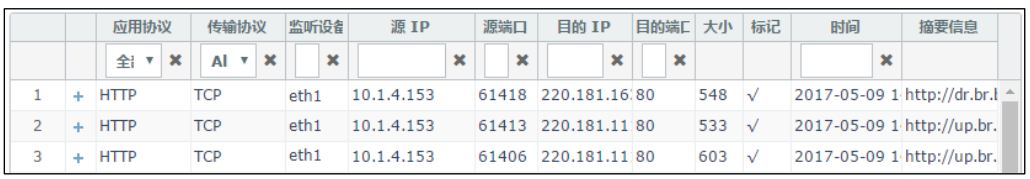
1. 选择**策略管理>内容检测**。
2. 点击**添加**，添加内容检测规则。

- 匹配标记：将匹配的内容进行标记，在网络审计中标记栏中可看到标记。
- 匹配丢弃：将匹配的内容进行丢弃，在网络审计中查看不到被丢弃的条目。

3. 点击**确定**。以同样方式添加更多内容检测规则。



配置成功后，数据流量命中“匹配标记”时，在**内容恢复**和**应用审计**中会标记出满足条件的条目。



3.6.IP 别名

为了方便管理员管理，NetEye IDS 提供了用户名称和 IP 地址绑定的功能，即在网络监控和审计结果中直接显示 IP 地址与用户名称的对应关系，无需管理员记忆和查找。

要配置用户绑定 IP，请以安全管理员的身份登录，并执行以下操作：

1. 选择**策略管理>用户 IP 设置**。
2. 点击**添加**，添加用户 IP。

3. 点击**确定**。以同样方式添加更多用户 IP。

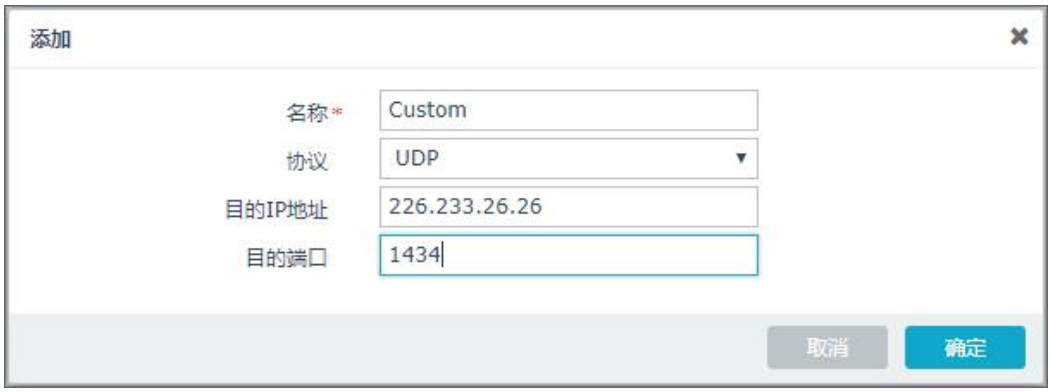
4. 可通过 IP 地址和用户名筛选绑定条目，点击右侧的 ✖ 可以清除筛选条件。

3.7.自定义协议

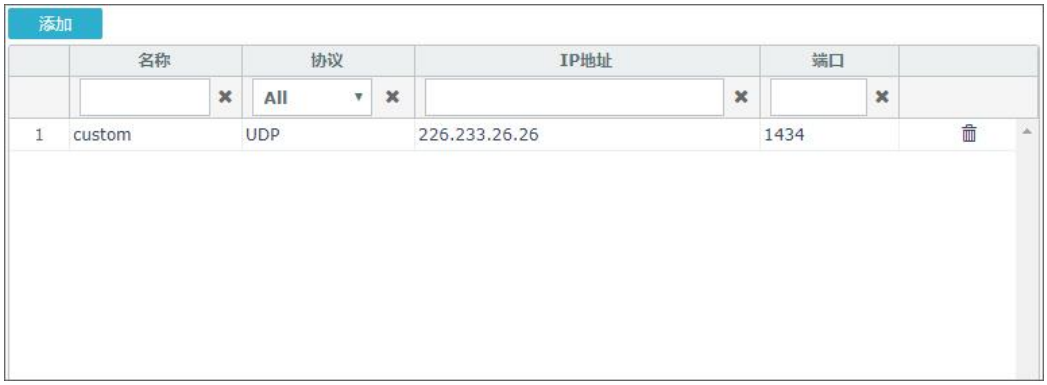
配置自定义协议功能后，系统会将管理员自定义的协议名称，分别显示在**实时报警**和**攻击检测**的列表中。

要配置自定义协议功能，请以安全管理员的身份登录，并执行以下操作：

1. 选择**策略管理>自定义协议**。
2. 点击**添加**，添加自定义协议内容。



3. 点击**确定**，以同样的方式可以添加更多自定义规则。



4. 可通过名称、协议、IP 地址和端口筛选条目，点击右侧的 可以清除筛选条件。

3.8.NEL 引擎

NEL 引擎为东软自主研发的一种通用攻击描述语言。能更加精准快速地识别出威胁。与 IDS 策略一同使用能够大幅提高系统威胁检测能力。

使用 NEL 引擎，需做如下配置，包括：

3.8.1. 常规设置

常规设置用来开启 NEL 检测引擎、引用已配置好的规则组，即防护配置，并确定该防护配置生效的网段。

要配置常规设置，请以安全管理员的身份登录，并执行以下操作：

1. 选择**策略管理> NEL 引擎>常规设置**。
2. 在引擎开关处，点击**开**。
3. 选择防护配置条目，设置是否开启 NEL 自定义规则，填写需进行防护的 IP 地址或 IP 地址段。

- 防护配置所选内容为在防护配置中所配置内容。
- 勾选启用自定义 NEL 规则表示系统匹配已配置的自定义规则。

4. 点击**确定**。

3.8.2. 防护配置

在此处配置防护规则组，用来被常规设置中引用使用。系统预定义了常用的规则组供您使用。只有在现有预定义的规则组不能满足需求时，才需自行创建。

要创建防护配置，请使用安全管理员身份登录系统，并执行如下操作：

1. 选择**策略> NEL 引擎>防护配置**。
2. 点击**新建**，根据需要进行配置。

3. 点击**确定**。

3.8.3. 自定义应用

此处可以为常见应用添加端口号。此处支持的应用有：HTTP、FTP、SMTP、POP3、IMAP、Oracle、Telnet、TFTP、DNS 和 SIP。如需为应用添加端口号请执行以下操作：

1. 选择**策略管理>NEL 引擎>自定义应用**。
2. 点击应用后面的  ，在弹出的对话框中配置。

3. 点击**确定**。

3.8.4. 规则库升级

定期升级规则库可以增强 NEL 引擎的检测能力。如需对规则库进行升级，请执行以下操作：

1. 选择**策略管理>NEL 引擎>规则库升级**。
2. 点击**上载规则库升级包**，手动上传本地保存的升级包至系统，点击**确定**，并重新登录系统。

3. 升级成功后，可在升级信息中查阅规则库升级相关信息。

3.9.AV 引擎

IDS 的 AV 引擎功能主要基于文件类型，对匹配客户端或服务器防护策略的数据流进行病毒扫描。如果检测到病毒，则根据安全管理员配置的动作进行处理（包括阻断或放行），并产生报警日志。

使用 AV 引擎，需做如下配置，包括：

3.9.1. 常规设置

常规设置用来开启 AV 检测引擎。

要配置常规设置，请以安全管理员的身份登录，并执行以下操作：

1. 选择**策略管理>AV 引擎>常规设置**。
2. 在引擎开关处，点击**开**。

3.9.2. 规则库升级

定期升级规则库可以增强 AV 引擎的检测能力。如需对规则库进行升级，请执行以下操作：

1. 选择**策略管理>AV 引擎>规则库升级**。
2. 点击**上载规则库升级包**，手动上传本地保存的升级包至系统，点击**确定**，并重新登录系统。

3. 升级成功后，可在升级信息中查阅规则库升级相关信息。

升级信息

引擎名称	引擎版本	规则版本	升级时间
Anti-Virus	0.0.1	1.0.447	2019-02-21 21:51:29

第4章 实时监控

入侵检测策略和监听接口配置完成后，安全管理员即可开始监控网络运行状态，包括：

- 4.1 实时报警
- 4.2 实时连接状态
- 4.3 实时数据流量
- 4.4 CPU 使用率
- 4.5 内存使用率

4.1.实时报警

安全管理员可通过实时报警页面即时查看网络中的入侵行为。开启了实时报警的事件被检测出时，系统会在界面右上角的实时报警快捷菜单处提示发生的攻击次数，管理员可以点击该快捷菜单跳转到实时报警页面查看实时报警信息。

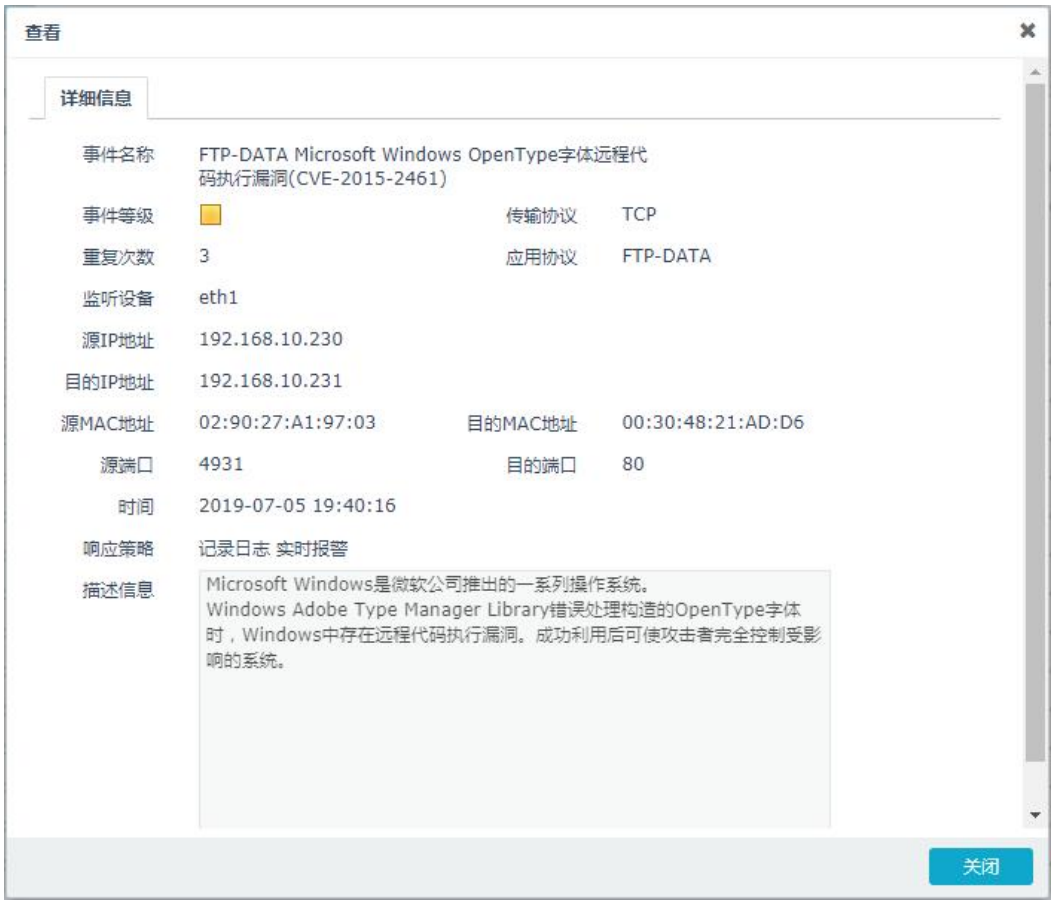
提示：安全管理员需要先在策略管理>策略配置页面开启实时报警功能并配置了监听接口。

要查看实时报警信息，请以安全管理员的身份登录，并执行以下操作：

1. 选择**实时监控>实时报警**。
2. 查看最新发生的攻击事件。

	事件名称	事件等级	重复次数	监听设备	传输协议	应用协议	源IP地址	目的IP地址	源端口	目的端口	时间
1	FTP-DATA Microsoft Word远程内存破坏漏洞(		9	eth1	IP	FTP-DATA	192.168.1.0	192.168.1.1	60000	2140	2019-07-05 19:28:53
2	FTP-DATA Adobe Flash Player内存破坏漏洞(		9	eth1	IP	FTP-DATA	192.168.1.0	192.168.1.1	60000	2140	2019-07-05 19:28:53
3	DNS Lion蠕虫		6	eth1	UDP	DNS	189.1.1.167	188.1.1.74	1264	53	2019-07-05 19:28:53
4	OTHER Quagga 0.98 和 0.99 版本的RIPd允		3	eth1	UDP	OTHER	192.168.13.1	255.255.255.25	520	520	2019-07-05 19:28:52
5	FTP-DATA Microsoft Windows OpenType字		3	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4970	80	2019-07-05 19:28:52
6	FTP-DATA Microsoft Windows OpenType字		3	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4969	80	2019-07-05 19:28:52
7	FTP-DATA Microsoft Windows OpenType字		3	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4968	80	2019-07-05 19:28:52
8	FTP-DATA Microsoft Windows OpenType字		3	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4967	80	2019-07-05 19:28:52
9	FTP-DATA Microsoft Windows OpenType字		3	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4966	80	2019-07-05 19:28:52
10	FTP-DATA Microsoft Windows OpenType字		2	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4934	80	2019-07-05 19:28:52
11	FTP-DATA Microsoft Windows OpenType字		2	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4933	80	2019-07-05 19:28:52
12	FTP-DATA Microsoft Windows OpenType字		2	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4932	80	2019-07-05 19:28:52
13	FTP-DATA Microsoft Windows OpenType字		2	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4931	80	2019-07-05 19:28:52
14	FTP-DATA Microsoft Windows OpenType字		2	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4930	80	2019-07-05 19:28:52
15	FTP-DATA Microsoft Windows OpenType字		2	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4925	80	2019-07-05 19:28:52
16	FTP-DATA Microsoft Windows OpenType字		2	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4924	80	2019-07-05 19:28:52
17	FTP-DATA Microsoft Windows OpenType字		2	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4923	80	2019-07-05 19:28:52
18	FTP-DATA Microsoft Windows OpenType字		2	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4922	80	2019-07-05 19:28:52
19	FTP-DATA Microsoft Windows OpenType字		2	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4921	80	2019-07-05 19:28:52
20	FTP-DATA Microsoft Windows OpenType字		2	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4907	80	2019-07-05 19:28:52
21	FTP-DATA Microsoft Windows OpenType字		3	eth1	TCP	FTP-DATA	192.168.10.23(	192.168.10.231	4906	80	2019-07-05 19:28:52

- 此页面只显示最新发生的攻击事件报警信息，最多显示 99 条。
- 点击主界面右上角的报警快捷菜单，也可跳转到此页面。主界面右上角的报警快捷菜单会实时提醒发生的攻击事件数量。
- 双击报警条目可以查看报警事件的详细信息。



- 点击攻击事件对应的🔍，可以跳转到**策略管理>策略配置**页面，查看或修改攻击事件的报警配置。
- 点击攻击事件对应的🗑，可以删除此条攻击事件的报警。

3. 点击**停止监视**按钮，可以停止实时报警的监视。
4. 点击**开始监视**按钮，可以开始实时报警的监视。
5. 点击**筛选**按钮，可以对攻击事件的报警信息按照**事件名称**、**事件等级**、**源 IP 地址**、**目的 IP 地址**、**源端口**、**目的端口**等条件进行筛选。

4.2.实时连接状态

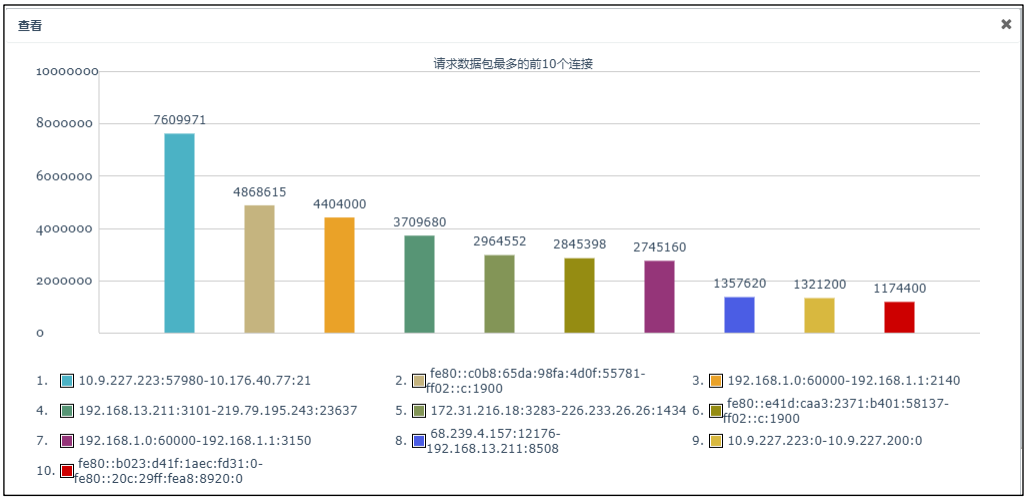
安全管理员可分类查看当前网络中监听到的网络连接的状态信息，还可以设置筛选条件、查看符合自定义条件的网络连接信息。

要查看实时连接状态，请以安全管理员的身份登录，并执行以下操作：

1. 选择**实时监控>实时连接状态**。
2. 查看实时的网络连接状态。

协议	连接状态	监听设备	源 IP	目的 IP	源端口	目的端口	请求字节数	应答字节数	时间	空闲时间（秒）
	All									
ICMP6	ICMP	eth1	fe80::b023:d41f:1ae	fe80::20c:29ff:fea8:			85120	85120	2019-02-01 10:56:24	0
ICMP	ICMP	eth1	10.9.227.223	10.9.227.200			95580	95580	2019-02-01 10:56:24	0
UDP	UDP	eth1	172.31.216.18	226.233.26.26	3283	1434	106656	0	2019-02-01 11:17:53	0
TCP	TCP_EST	eth1	192.168.1.111	192.168.2.222	1915	53	692	0	2019-02-01 10:56:25	181
TCP	TCP_EST	eth1	10.9.227.223	10.176.40.77	57980	21	271138	445384	2019-02-01 10:56:22	182
TCP	TCP_EST	eth1	192.168.1.111	192.168.2.222	6704	139	716	0	2019-02-01 10:56:26	289
TCP	TCP_EST	eth1	192.168.1.111	192.168.2.222	3901	1433	540	0	2019-02-01 10:56:25	290
TCP	TCP_EST	eth1	192.168.13.211	125.33.125.1	3132	20957	0	0	2019-02-01 10:56:23	292
TCP	TCP_EST	eth1	192.168.13.211	125.33.124.152	3133	7648	478	0	2019-02-01 10:56:23	292
TCP	TCP_EST	eth1	192.168.13.211	211.98.170.163	3135	2568	412	0	2019-02-01 10:56:23	292
TCP	TCP_EST	eth1	192.168.13.211	211.98.170.163	3134	2569	408	0	2019-02-01 10:56:23	292
TCP	TCP_EST	eth1	192.168.13.211	211.98.170.163	3131	2565	412	0	2019-02-01 10:56:23	292
TCP	TCP_EST	eth1	192.168.13.211	211.98.170.163	3130	2567	412	0	2019-02-01 10:56:23	292
TCP	TCP_EST	eth1	192.168.13.211	211.98.170.163	3120	2568	412	0	2019-02-01 10:56:23	292
TCP	TCP_EST	eth1	192.168.13.211	219.79.195.243	3101	23637	154160	906572	2019-02-01 10:56:23	292
TCP	TCP_EST	eth1	192.168.13.211	125.33.125.1	3128	20957	410	0	2019-02-01 10:56:23	292
TCP	TCP_EST	eth1	192.168.13.211	211.98.170.163	3129	2568	408	0	2019-02-01 10:56:23	292
TCP	TCP_EST	eth1	192.168.13.211	211.98.170.163	3127	2565	412	0	2019-02-01 10:56:23	292

- 连接状态包括 ICMP、UDP、TCP_SYN_SENT、TCP_SYN_RCVD、TCP_EST、TCP_CLOSE 和 All。
- 可通过连接状态、源和目的 IP 地址、源和目的端口筛选查看的连接信息，点击右侧的 ✖ 可以清除筛选条件。
- 实时连接超过 100 条时将分页显示，通过页码前后的箭头可以翻页查看。
- 点击“请求字节数”等表头项后的 📊，可以查看此类流量的 Top10 连接排名。



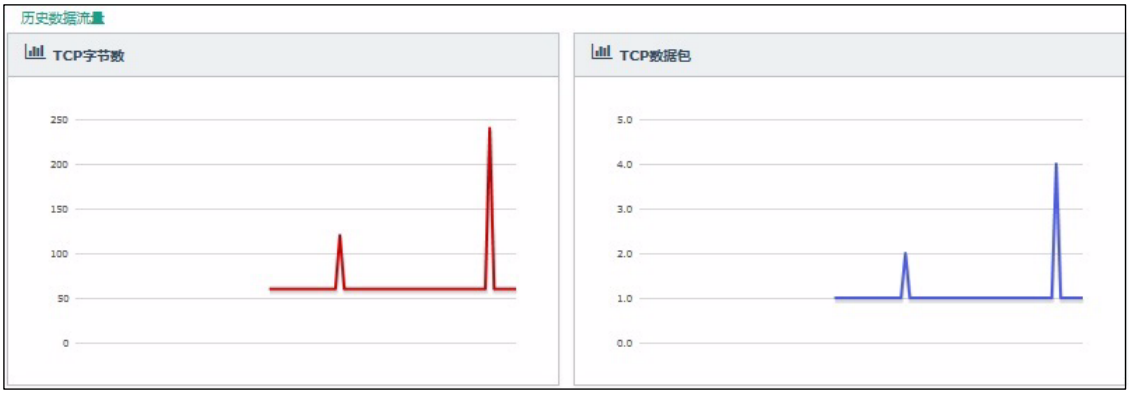
- 点击列表左下方的，可以设置偏好设置。勾选置灰的条目后点击**确定**，对应的信息将会出现在实时连接查看列表中。

4.3.实时数据流量

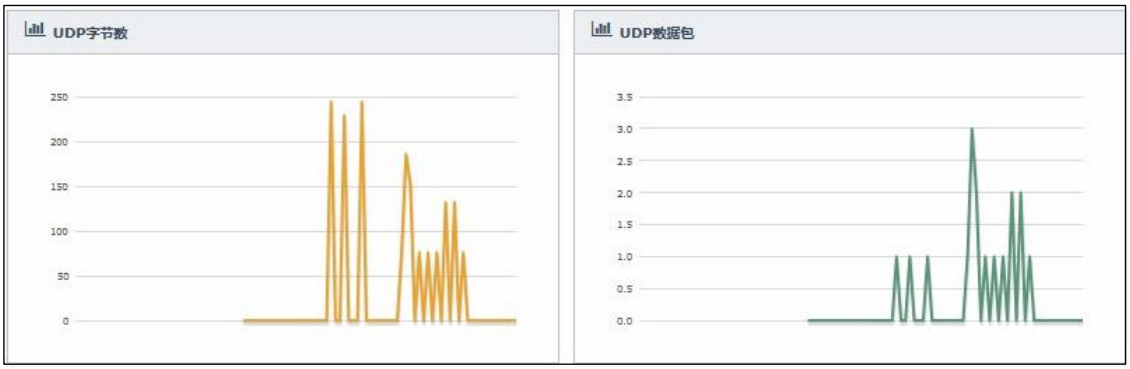
安全管理员可通过折线图查看当前网络中可监听到的实时数据流量，包括 TCP、UDP、ICMP 三种协议的数据。

要查看实时数据流量，请以安全管理员的身份登录，并执行以下操作：

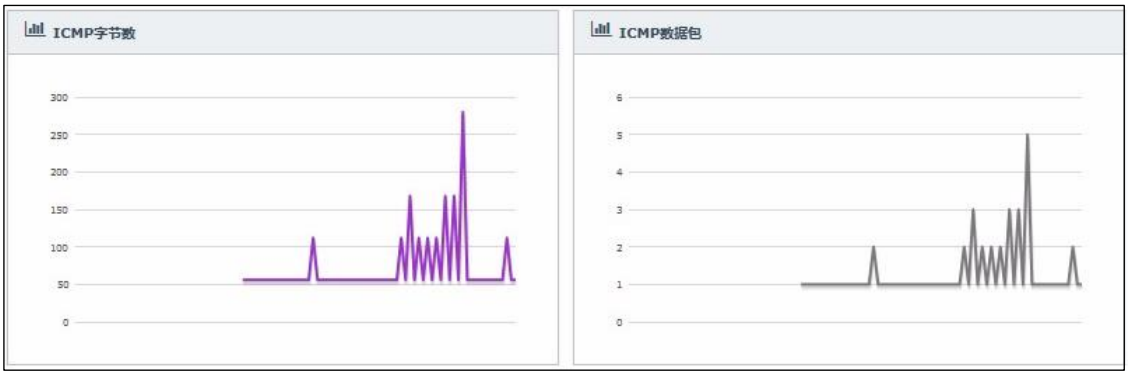
1. 选择**实时监控>实时数据流量**。
2. 查看实时的全局网络流量信息，包括：
   - TCP 字节数和数据包数



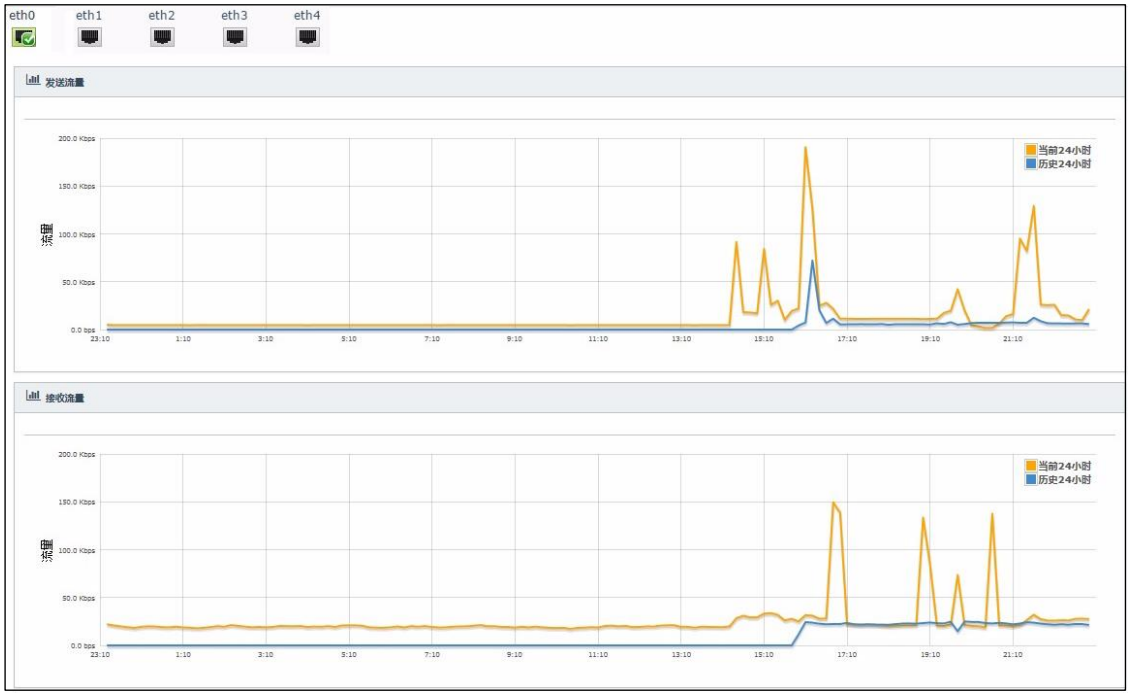
   - UDP 字节数和数据包数



   - ICMP 字节数和数据包数



3. 点击**历史数据流量页签**，可以查看接口接收和发送的历史数据流量信息。

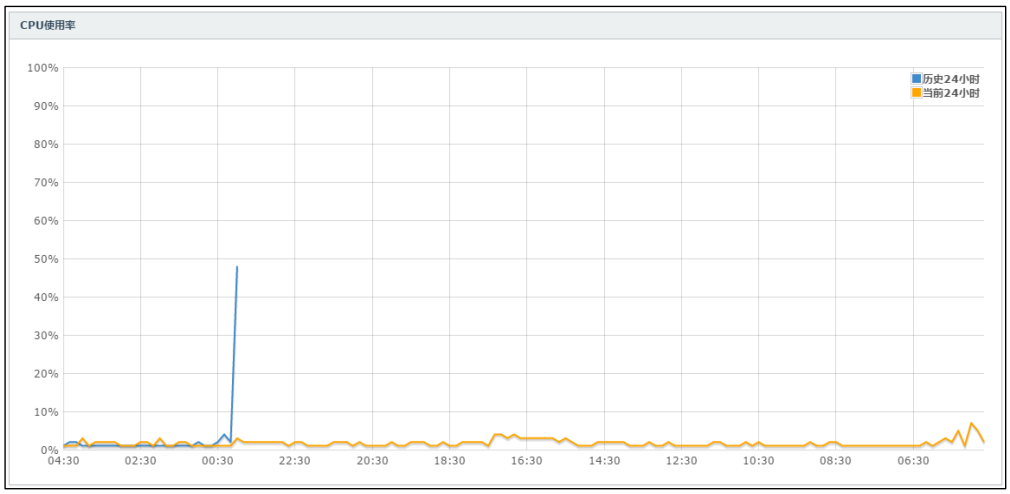


4.4.CPU 使用率

安全管理员可以通过此功能了解设备的 CPU 使用率。

要查看 CPU 使用率，请以安全管理员的身份登录，并执行以下操作：

1. 选择**实时监控>CPU 使用率。**
2. 查看实时的 CPU 使用率情况。

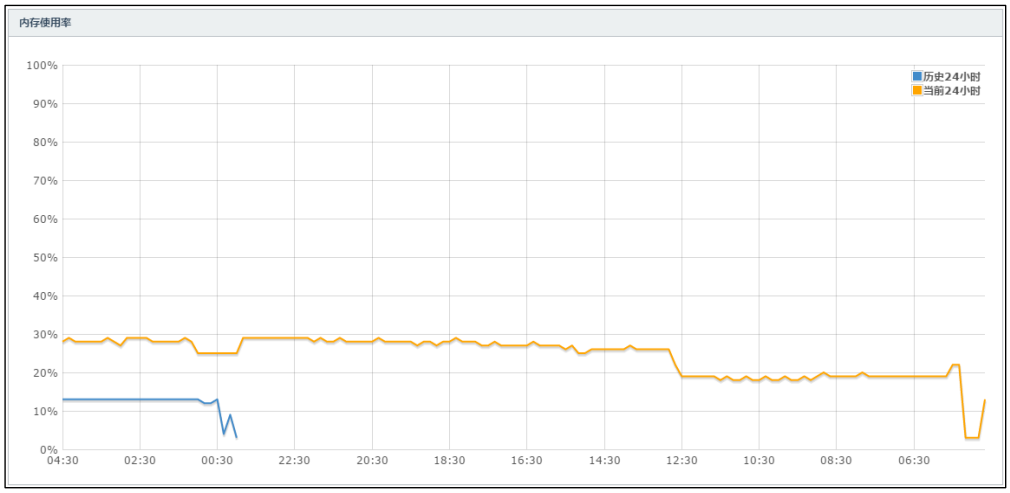


4.5.内存使用率

安全管理员可以通过此功能了解设备的内存使用率。

要查看内存使用率，请以安全管理员的身份登录，并执行以下操作：

1. 选择**实时监控>内存使用率。**
2. 查看实时的内存使用率情况。



第5章 网络审计

安全管理员可以查看网络审计信息，包括：

5.1.攻击检测

如果在**策略管理>策略配置**中开启记录日志功能，安全管理员可通过**攻击检测**页面查看全部攻击事件。

要查看攻击事件，请以安全管理员身份登录，并执行以下操作：

1. 选择**网络审计>攻击检测**。
2. 查看攻击事件。

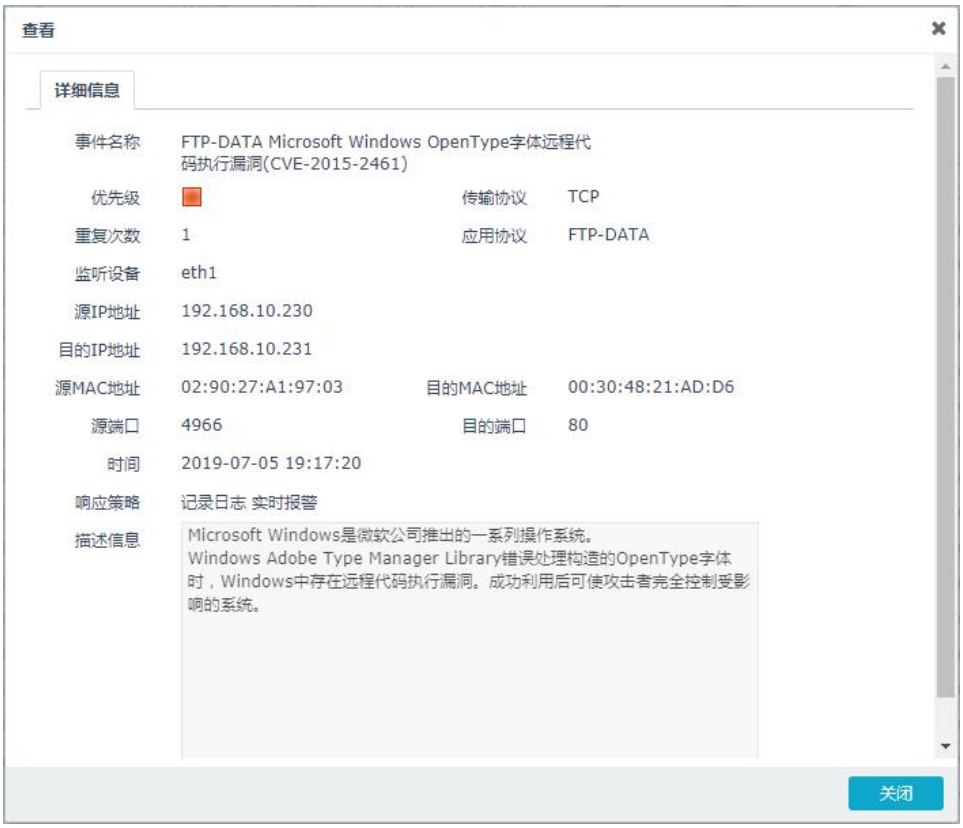
	事件名称	事件等级	监听设备	传输协议	应用协议	源 IP	源端口	目的 IP	目的端口	重复次数	时间
		全部		All							
1	FTP-DATA Microsoft Word远程		eth1	IP	FTP-DATA	192.168.1.0	60000	192.168.1.1	2140	3	2019-07-05 19:17:21
2	FTP-DATA Adobe Flash Playe		eth1	IP	FTP-DATA	192.168.1.0	60000	192.168.1.1	2140	3	2019-07-05 19:17:21
3	DNS Lion蠕虫		eth1	UDP	DNS	189.1.1.167	1264	188.1.1.74	53	2	2019-07-05 19:17:21
4	OTHER Quagga 0.98 和 0.99		eth1	UDP	OTHER	192.168.13.1	520	255.255.255.255	520	1	2019-07-05 19:17:21
5	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4970	192.168.10.231	80	1	2019-07-05 19:17:20
6	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4969	192.168.10.231	80	1	2019-07-05 19:17:20
7	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4968	192.168.10.231	80	1	2019-07-05 19:17:20
8	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4967	192.168.10.231	80	1	2019-07-05 19:17:20
9	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4966	192.168.10.231	80	1	2019-07-05 19:17:20
10	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4934	192.168.10.231	80	1	2019-07-05 19:17:20
11	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4933	192.168.10.231	80	1	2019-07-05 19:17:20
12	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4932	192.168.10.231	80	1	2019-07-05 19:17:20
13	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4931	192.168.10.231	80	1	2019-07-05 19:17:20
14	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4930	192.168.10.231	80	1	2019-07-05 19:17:20
15	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4925	192.168.10.231	80	1	2019-07-05 19:17:20
16	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4924	192.168.10.231	80	1	2019-07-05 19:17:20
17	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4923	192.168.10.231	80	1	2019-07-05 19:17:20
18	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4922	192.168.10.231	80	1	2019-07-05 19:17:20
19	FTP-DATA Microsoft Windows		eth1	TCP	FTP-DATA	192.168.10.230	4921	192.168.10.231	80	1	2019-07-05 19:17:20
20	POP3 SketchUp 内存破坏和缓		eth1	TCP	POP3	192.168.1.50	80	192.168.1.117	3919	1	2019-07-05 19:17:19
21	SMTP Microsoft Windows Tru		eth1	TCP	SMTP	192.168.1.50	80	192.168.1.117	3919	1	2019-07-05 19:17:19

第 1 页 100

- 可通过事件等级、监听设备、源 IP 和端口、目的 IP 和端口、时间（事件发生时间）筛选查看的网络攻击事件，点击右侧的 ✖ 可以清除筛选条件。
- 攻击事件超过 100 条时，使用页面下方的下拉菜单可以选择每页显示条目数，超过选中条目数时分页显示，通过页码前后的箭头可以翻页查看。

- 点击页面左下角的，可以设置偏好设置。勾选置灰的条目后点击**确定**，对应的信息将会出现在攻击事件查看列表中。

- 双击条目可以查看攻击事件的详细信息。

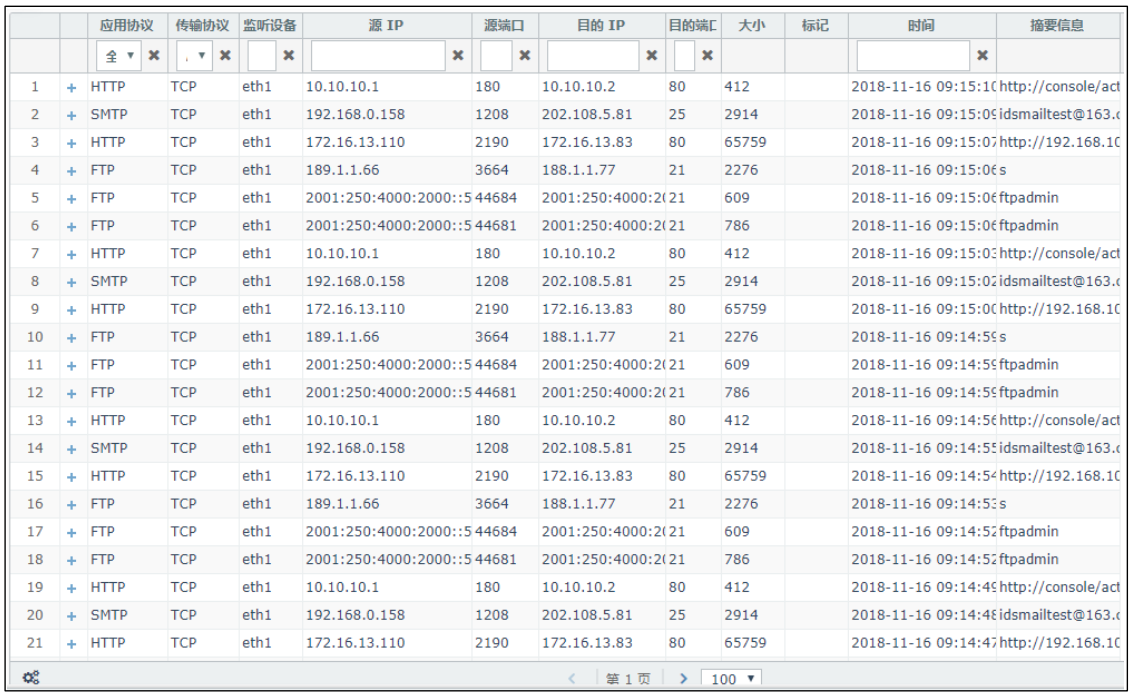


5.2.内容恢复

安全管理员可通过**内容恢复**页面查看 NetEye IDS 监听到的内容。

要查看恢复的内容，请以安全管理员身份登录，并执行以下操作：

1. 选择**网络审计>内容恢复**。
2. 查看内容恢复概要信息。

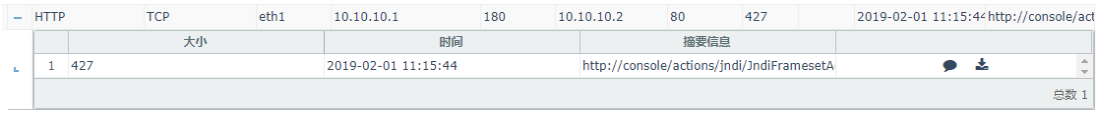


		应用协议	传输协议	监听设备	源 IP	源端口	目的 IP	目的端口	大小	标记	时间	摘要信息
		全										
1	+	HTTP	TCP	eth1	10.10.10.1	180	10.10.10.2	80	412		2018-11-16 09:15:1(	http://console/act
2	+	SMTP	TCP	eth1	192.168.0.158	1208	202.108.5.81	25	2914		2018-11-16 09:15:0(	idsmailtest@163.(
3	+	HTTP	TCP	eth1	172.16.13.110	2190	172.16.13.83	80	65759		2018-11-16 09:15:07	http://192.168.1(
4	+	FTP	TCP	eth1	189.1.1.66	3664	188.1.1.77	21	2276		2018-11-16 09:15:06	s
5	+	FTP	TCP	eth1	2001:250:4000:2000::5	44684	2001:250:4000:2(	21	609		2018-11-16 09:15:06	ftpadmin
6	+	FTP	TCP	eth1	2001:250:4000:2000::5	44681	2001:250:4000:2(	21	786		2018-11-16 09:15:06	ftpadmin
7	+	HTTP	TCP	eth1	10.10.10.1	180	10.10.10.2	80	412		2018-11-16 09:15:03	http://console/act
8	+	SMTP	TCP	eth1	192.168.0.158	1208	202.108.5.81	25	2914		2018-11-16 09:15:02	idsmailtest@163.(
9	+	HTTP	TCP	eth1	172.16.13.110	2190	172.16.13.83	80	65759		2018-11-16 09:15:0(	http://192.168.1(
10	+	FTP	TCP	eth1	189.1.1.66	3664	188.1.1.77	21	2276		2018-11-16 09:14:59	s
11	+	FTP	TCP	eth1	2001:250:4000:2000::5	44684	2001:250:4000:2(	21	609		2018-11-16 09:14:59	ftpadmin
12	+	FTP	TCP	eth1	2001:250:4000:2000::5	44681	2001:250:4000:2(	21	786		2018-11-16 09:14:59	ftpadmin
13	+	HTTP	TCP	eth1	10.10.10.1	180	10.10.10.2	80	412		2018-11-16 09:14:56	http://console/act
14	+	SMTP	TCP	eth1	192.168.0.158	1208	202.108.5.81	25	2914		2018-11-16 09:14:55	idsmailtest@163.(
15	+	HTTP	TCP	eth1	172.16.13.110	2190	172.16.13.83	80	65759		2018-11-16 09:14:54	http://192.168.1(
16	+	FTP	TCP	eth1	189.1.1.66	3664	188.1.1.77	21	2276		2018-11-16 09:14:53	s
17	+	FTP	TCP	eth1	2001:250:4000:2000::5	44684	2001:250:4000:2(	21	609		2018-11-16 09:14:52	ftpadmin
18	+	FTP	TCP	eth1	2001:250:4000:2000::5	44681	2001:250:4000:2(	21	786		2018-11-16 09:14:52	ftpadmin
19	+	HTTP	TCP	eth1	10.10.10.1	180	10.10.10.2	80	412		2018-11-16 09:14:49	http://console/act
20	+	SMTP	TCP	eth1	192.168.0.158	1208	202.108.5.81	25	2914		2018-11-16 09:14:48	idsmailtest@163.(
21	+	HTTP	TCP	eth1	172.16.13.110	2190	172.16.13.83	80	65759		2018-11-16 09:14:47	http://192.168.1(

第 1 页 100

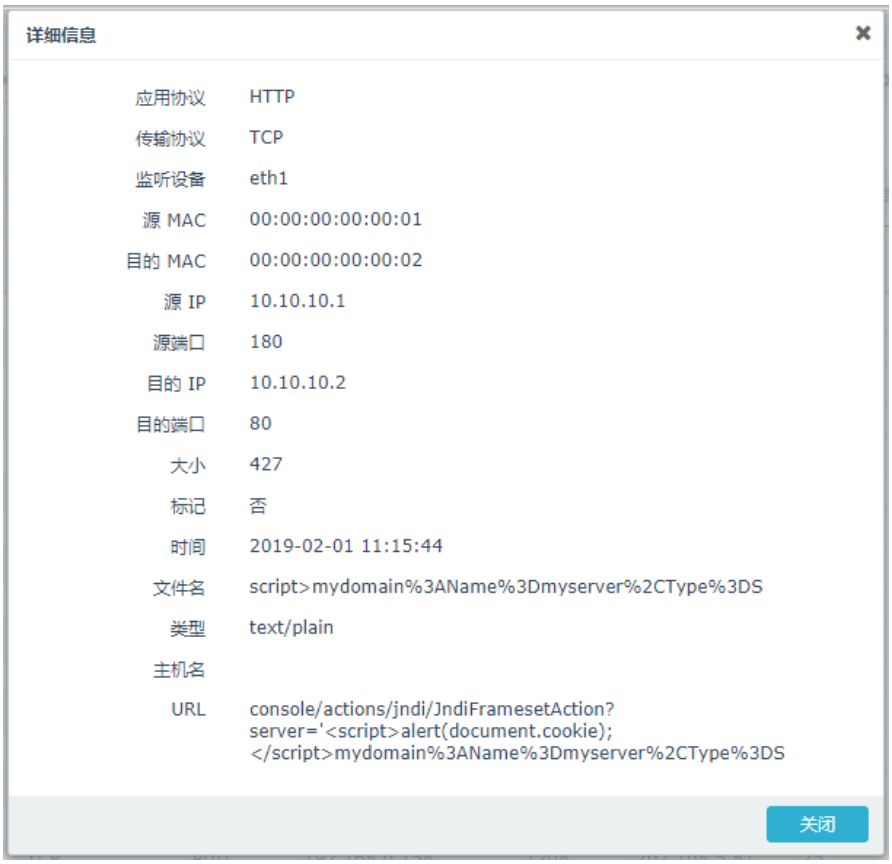
- 可通过应用协议、传输协议、监听设备、源 IP、源端口、目的 IP、目的端口和用户访问时间对记录进行筛选，点击右侧的 ✖ 可以清除筛选条件。
- 内容条目超过 100 条时，使用页面下方的下拉菜单可以选择每页显示条目数，超过选中条目数时分页显示，通过页码前后的箭头可以翻页查看。
- 点击页面左下角的 ⚙，可以设置偏好设置。勾选置灰的条目后点击**确定**，对应的信息将会出现在内容恢复查看列表中。

3. 点击条目前“+”，显示折叠内容。

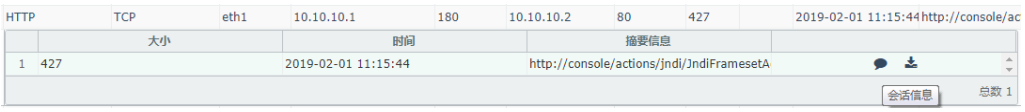


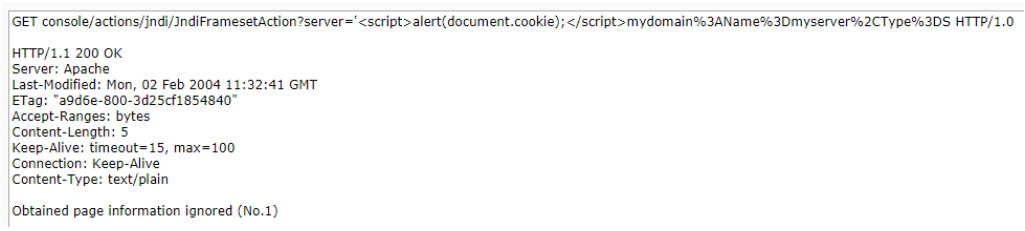
4. 双击展开的条目，显示详细信息。

- 显示如下内容。

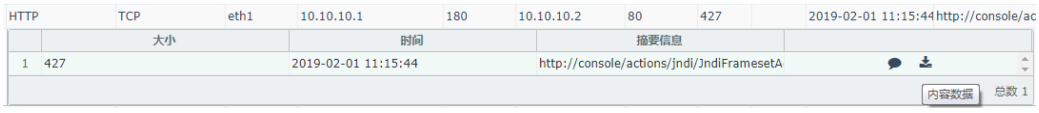


- 点击会话信息图标显示如下内容。





- 点击内容数据图标，会将数据下载到本地管理主机，供近一步分析。

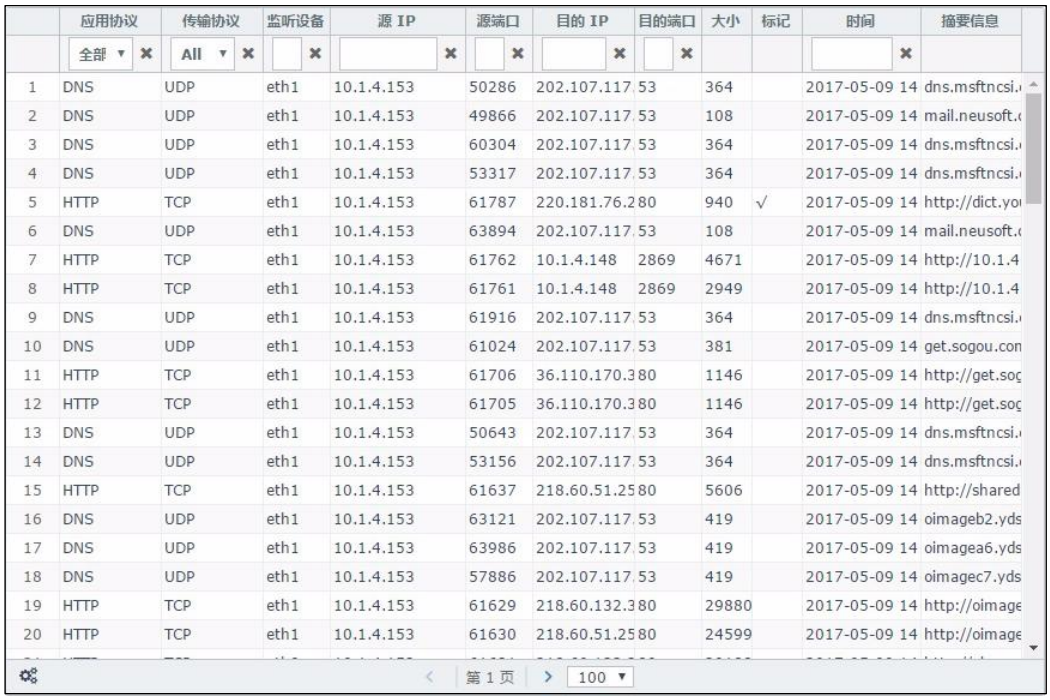


5.3.应用审计

安全管理员可通过**应用审计**页面查看 NetEye IDS 监控到的全部应用信息。

要查看应用信息，请以安全管理员身份登录，并执行以下操作：

1. 选择**网络审计>应用审计**。
2. 查看网络中的应用信息。



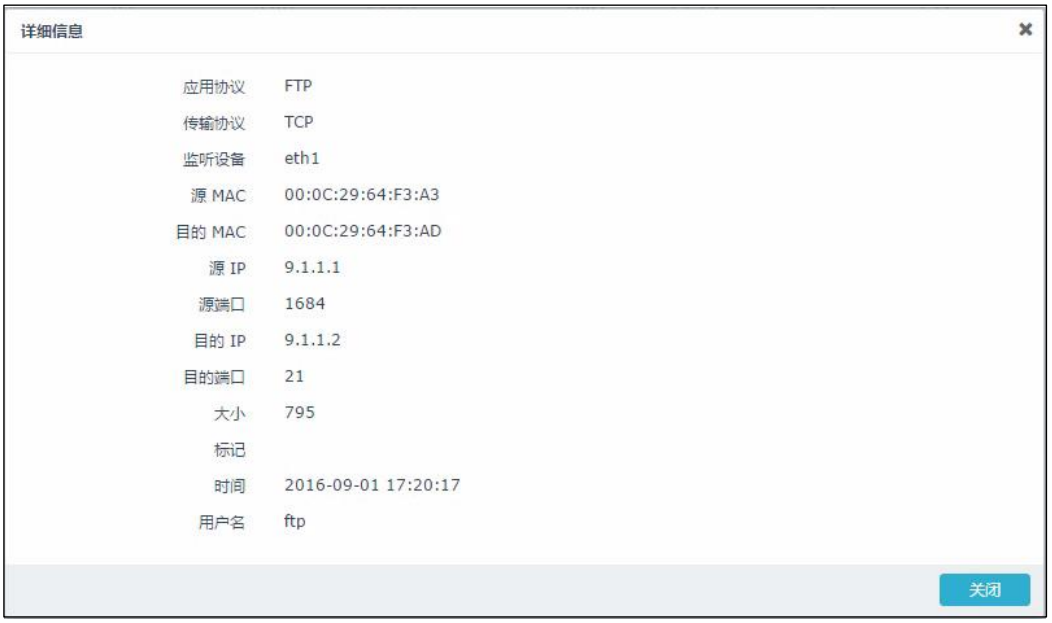
	应用协议	传输协议	监听设备	源 IP	源端口	目的 IP	目的端口	大小	标记	时间	摘要信息
	全部	All									
1	DNS	UDP	eth1	10.1.4.153	50286	202.107.117	53	364		2017-05-09 14	dns.msftncsi.
2	DNS	UDP	eth1	10.1.4.153	49866	202.107.117	53	108		2017-05-09 14	mail.neusoft.
3	DNS	UDP	eth1	10.1.4.153	60304	202.107.117	53	364		2017-05-09 14	dns.msftncsi.
4	DNS	UDP	eth1	10.1.4.153	53317	202.107.117	53	364		2017-05-09 14	dns.msftncsi.
5	HTTP	TCP	eth1	10.1.4.153	61787	220.181.76.2	80	940	√	2017-05-09 14	http://dict.yo
6	DNS	UDP	eth1	10.1.4.153	63894	202.107.117	53	108		2017-05-09 14	mail.neusoft.
7	HTTP	TCP	eth1	10.1.4.153	61762	10.1.4.148	2869	4671		2017-05-09 14	http://10.1.4
8	HTTP	TCP	eth1	10.1.4.153	61761	10.1.4.148	2869	2949		2017-05-09 14	http://10.1.4
9	DNS	UDP	eth1	10.1.4.153	61916	202.107.117	53	364		2017-05-09 14	dns.msftncsi.
10	DNS	UDP	eth1	10.1.4.153	61024	202.107.117	53	381		2017-05-09 14	get.sogou.com
11	HTTP	TCP	eth1	10.1.4.153	61706	36.110.170.3	80	1146		2017-05-09 14	http://get.sog
12	HTTP	TCP	eth1	10.1.4.153	61705	36.110.170.3	80	1146		2017-05-09 14	http://get.sog
13	DNS	UDP	eth1	10.1.4.153	50643	202.107.117	53	364		2017-05-09 14	dns.msftncsi.
14	DNS	UDP	eth1	10.1.4.153	53156	202.107.117	53	364		2017-05-09 14	dns.msftncsi.
15	HTTP	TCP	eth1	10.1.4.153	61637	218.60.51.25	80	5606		2017-05-09 14	http://shared
16	DNS	UDP	eth1	10.1.4.153	63121	202.107.117	53	419		2017-05-09 14	oimageb2.yds
17	DNS	UDP	eth1	10.1.4.153	63986	202.107.117	53	419		2017-05-09 14	oimagea6.yds
18	DNS	UDP	eth1	10.1.4.153	57886	202.107.117	53	419		2017-05-09 14	oimagec7.yds
19	HTTP	TCP	eth1	10.1.4.153	61629	218.60.132.3	80	29880		2017-05-09 14	http://oimage
20	HTTP	TCP	eth1	10.1.4.153	61630	218.60.51.25	80	24599		2017-05-09 14	http://oimage

第 1 页 100

- 应用协议：支持 HTTP、TELNET、FTP、SMTP、POP3 等。
- 标记：表示该条记录命中了**策略管理>内容检测**所配置的标记条件。
- 摘要信息：表示该条目信息的简要说明，如，该条目为 HTTP 协议，此处显示访问的 URL 地址。
- 可通过应用协议、传输协议、监听设备、源 IP 和端口、目的 IP 和端口、时间（用户访问应用的时间）筛选查看应用信息，点击右侧的 ✖ 可以清除筛选条件。
- 审计应用超过 100 条时，使用页面下方的下拉菜单可以选择每页显示条目数，超过选中条目数时分页显示，通过页码前后的箭头可以翻页查看。

- 点击页面左下角的，可以进行偏好设置。勾选置灰的条目后点击**确定**，对应的信息将会出现在应用审计查看列表中。

- 双击条目可以查看审计应用的详细信息。



5.4.连接审计

安全管理员可通过**连接审计**页面查看 NetEye IDS 监控到的全部连接信息。

要查看连接信息，请以安全管理员身份登录，并执行以下操作：

1. 选择**网络审计>连接审计**。
2. 查看网络中的连接信息。

传输协议	连接状态	监听设备	源 IP	目的 IP	目的端口	连接次数	请求字节数	应答字节数	时间
All									
TCP	TCP_SYN_SENT	eth1	192.168.10.230	192.168.10.230	80	4	0	0	2018-11-16 09:23:05
TCP	TCP_CLOSE	eth1	192.168.13.211	192.168.13.211	20957	4	1644	916	2018-11-16 09:22:57
TCP	TCP_CLOSE	eth1	192.168.13.211	192.168.13.211	19999	3	1437	687	2018-11-16 09:22:57
TCP	TCP_CLOSE	eth1	192.168.13.211	192.168.13.211	2570	2	824	0	2018-11-16 09:22:57
TCP	TCP_CLOSE	eth1	192.168.13.211	192.168.13.211	2565	11	824	0	2018-11-16 09:22:57
TCP	TCP_CLOSE	eth1	192.168.13.211	192.168.13.211	2567	11	2051	0	2018-11-16 09:22:57
TCP	TCP_CLOSE	eth1	192.168.13.211	192.168.13.211	2571	2	0	0	2018-11-16 09:22:57
TCP	TCP_CLOSE	eth1	192.168.13.211	192.168.13.211	18838	6	0	0	2018-11-16 09:22:57
TCP	TCP_CLOSE	eth1	192.168.13.211	192.168.13.211	16255	5	0	0	2018-11-16 09:22:57
TCP	TCP_CLOSE	eth1	192.168.13.211	192.168.13.211	18941	10	0	0	2018-11-16 09:22:57
TCP	TCP_CLOSE	eth1	192.168.13.211	192.168.13.211	8080	3	1650	3564	2018-11-16 09:22:57
TCP	TCP_CLOSE	eth1	192.168.13.211	192.168.13.211	8080	4	1924	4752	2018-11-16 09:22:57
TCP	TCP_CLOSE	eth1	192.168.13.211	192.168.13.211	80	4	2644	896	2018-11-16 09:22:57
TCP	TCP_CLOSE	eth1	192.168.0.158	192.168.0.158	25	4	11920	3000	2018-11-16 09:22:56
TCP	TCP_CLOSE	eth1	1.1.51.86	1.1.51.86	1094	4	944	400	2018-11-16 09:22:56
TCP	TCP_SYN_RECV	eth1	192.168.10.238	192.168.10.238	143	2	0	0	2018-11-16 09:22:55
TCP	TCP_CLOSE	eth1	192.168.10.238	192.168.10.238	143	389	77455	118947	2018-11-16 09:22:55
TCP	TCP_CLOSE	eth1	172.16.13.110	172.16.13.110	80	4	539680	608	2018-11-16 09:22:55

第 1 页　100

- 可通过传输协议、监听设备、源 IP、目的 IP 和端口以及时间（即连接建立时间）筛选查看的连接信息，点击右侧的 ✖ 可以清除筛选条件。
- 审计连接超过 100 条时，使用页面下方的下拉菜单可以选择每页显示条目数，超过选中条目数时分页显示，通过页码前后的箭头可以翻页查看。

- 点击页面左下角的，可以设置偏好设置。勾选置灰的条目后点击**确定**，对应的信息将会出现在连接审计查看列表中。

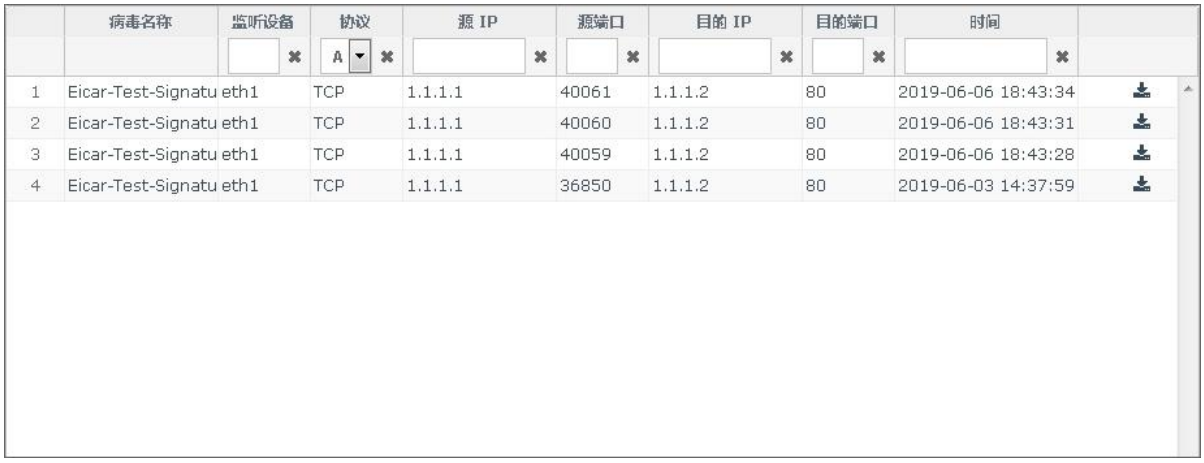
- 双击条目可以查看审计连接的详细信息。

5.5.AV 报警

安全管理员可通过 **AV 报警**页面查看 NetEyeIDS 监控到的 AV 报警信息。

要查看 AV 报警信息，请以安全管理员身份登录，并执行以下操作：

1. 选择**网络审计>AV 报警。**
2. 查看网络中的 AV 报警信息。



	病毒名称	监听设备	协议	源 IP	源端口	目的 IP	目的端口	时间	
1	Eicar-Test-Signatu	eth1	TCP	1.1.1.1	40061	1.1.1.2	80	2019-06-06 18:43:34	
2	Eicar-Test-Signatu	eth1	TCP	1.1.1.1	40060	1.1.1.2	80	2019-06-06 18:43:31	
3	Eicar-Test-Signatu	eth1	TCP	1.1.1.1	40059	1.1.1.2	80	2019-06-06 18:43:28	
4	Eicar-Test-Signatu	eth1	TCP	1.1.1.1	36850	1.1.1.2	80	2019-06-03 14:37:59	

- 可通过监听设备、协议、源 IP、源端口、目的 IP、目的端口及时间，筛选查看 AV 报警信息，点击右侧的 ✖ 可以清除筛选条件。
- AV 报警信息超过 100 条时，使用页面下方的下拉菜单可以选择每页显示条目数，超过选中条目数时分页显示，通过页码前后的箭头可以翻页查看。
- 点击页面左下角的 ⚙，可以设置偏好设置。勾选置灰的条目后点击**确定**，对应的信息将会出现在查看列表中。

- 双击条目可以查看 AV 报警的详细信息。

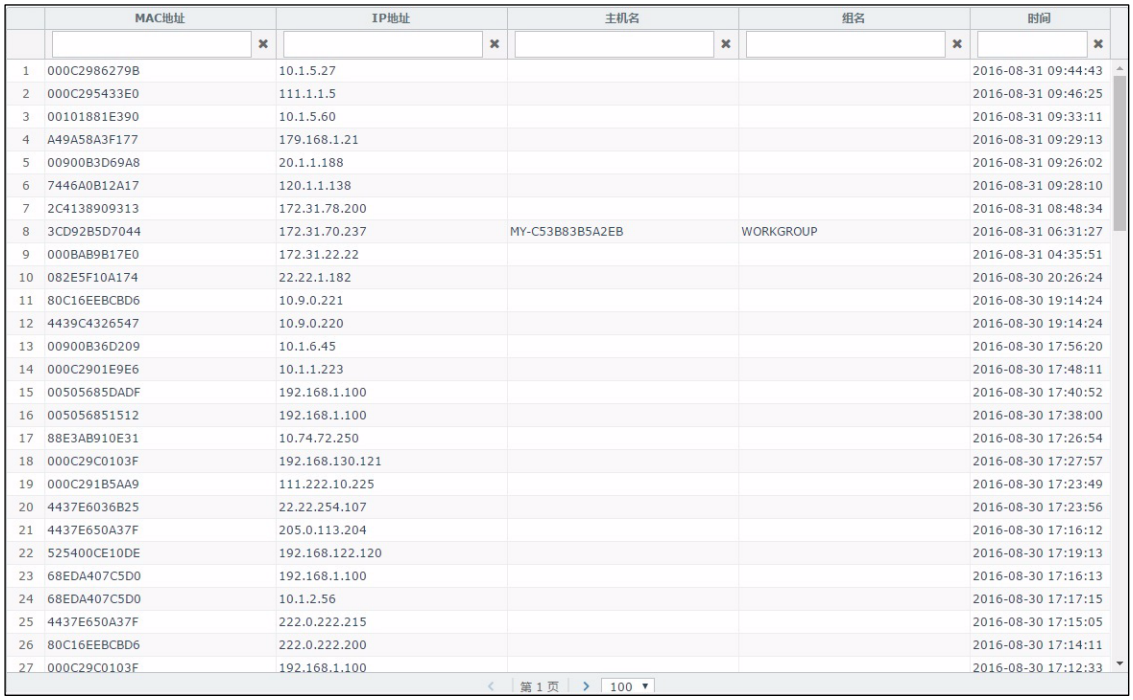

查看
详细信息
病毒名称 Eicar-Test-Signature.UNOFFICIAL FOUND
监听设备 eth1
协议 TCP
源IP地址 1.1.1.1
目的IP地址 1.1.1.2
源MAC地址 00:0C:29:D3:19:F0
目的MAC地址 00:0C:29:5C:7B:87
源端口 40061
目的端口 80
时间 2019-06-06 18:43:34
关闭

5.6.网络信息收集

NetEye IDS 收集与监听口相连的网络（即监听网络）内的所有主机网络信息。

要查看 NetEye IDS 收集的网络信息，请以安全管理员身份登录，并执行以下操作：

1. 选择**网络审计>网络信息收集**。
2. 查看监听网络中的主机信息。



	MAC地址	IP地址	主机名	组名	时间
1	000C2986279B	10.1.5.27			2016-08-31 09:44:43
2	000C295433E0	111.1.1.5			2016-08-31 09:46:25
3	00101881E390	10.1.5.60			2016-08-31 09:33:11
4	A49A58A3F177	179.168.1.21			2016-08-31 09:29:13
5	00900B3D69A8	20.1.1.188			2016-08-31 09:26:02
6	7446A0B12A17	120.1.1.138			2016-08-31 09:28:10
7	2C4138909313	172.31.78.200			2016-08-31 08:48:34
8	3CD92B5D7044	172.31.70.237	MY-C53B83B5A2EB	WORKGROUP	2016-08-31 06:31:27
9	000BAB9B17E0	172.31.22.22			2016-08-31 04:35:51
10	082E5F10A174	22.22.1.182			2016-08-30 20:26:24
11	80C16EEBCBD6	10.9.0.221			2016-08-30 19:14:24
12	4439C4326547	10.9.0.220			2016-08-30 19:14:24
13	00900B36D209	10.1.6.45			2016-08-30 17:56:20
14	000C2901E9E6	10.1.1.223			2016-08-30 17:48:11
15	00505685DADF	192.168.1.100			2016-08-30 17:40:52
16	005056851512	192.168.1.100			2016-08-30 17:38:00
17	88E3AB910E31	10.74.72.250			2016-08-30 17:26:54
18	000C29C0103F	192.168.130.121			2016-08-30 17:27:57
19	000C291B5AA9	111.222.10.225			2016-08-30 17:23:49
20	4437E6036B25	22.22.254.107			2016-08-30 17:23:56
21	4437E650A37F	205.0.113.204			2016-08-30 17:16:12
22	525400CE10DE	192.168.122.120			2016-08-30 17:19:13
23	68EDA407C5D0	192.168.1.100			2016-08-30 17:16:13
24	68EDA407C5D0	10.1.2.56			2016-08-30 17:17:15
25	4437E650A37F	222.0.222.215			2016-08-30 17:15:05
26	80C16EEBCBD6	222.0.222.200			2016-08-30 17:14:11
27	000C29C0103F	192.168.1.100			2016-08-30 17:12:33

第 1 页 100

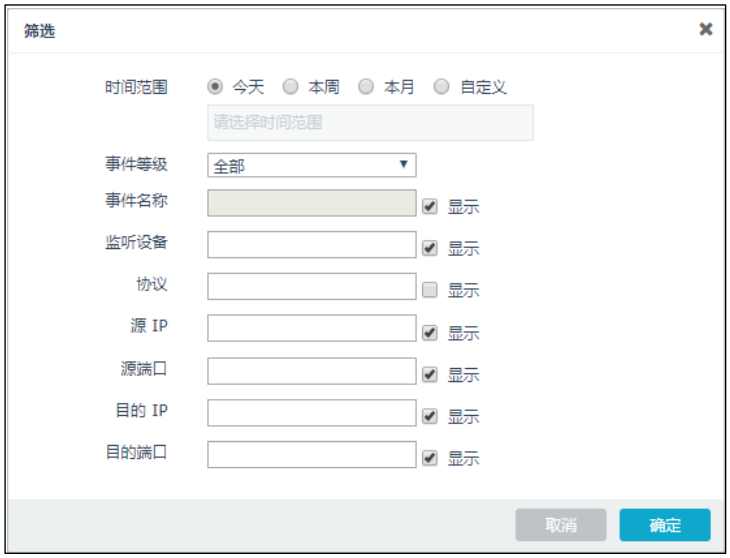
- 可通过 MAC 地址、IP 地址、主机名、组名（主机所在工作组名称）、时间（主机信息最后更新时间）筛选查看的主机信息，点击右侧的 ✖ 可以清除筛选条件。
- 主机信息超过 100 条时，使用页面下方的下拉菜单可以选择每页显示条目数，超过选中条目数时分页显示，通过页码前后的箭头可以翻页查看。

5.7.攻击统计

安全管理员可在此查看攻击统计情况，统计时间区间支持今天、本周、本月和自定义。同时可选择统计信息的表头显示项。并可对各显示项设置筛选条件，查看符合自定义条件的攻击信息。

要查看攻击统计，请以安全管理员的身份登录，并执行以下操作：

1. 选择**网络审计>攻击统计**。
2. 点击**筛选**，选择显示内容并填写筛选条件。



- 时间范围：缺省情况下，显示今天受攻击情况。可选择**今天**、**本周**、**本月**和**自定义**。选择自定义后，需指定时间区间。
- 事件等级：事件等级包括：**全部**、**高**、**中**、**低**和**预警信息**。
- 显示：可选择勾选或者不勾选，在此处选择统计列表的显示项，同时也是筛选依据。包括：事件名称、监听设备、协议、源 IP、源端口、目的 IP 和目的端口。在显示的表格中，事件等级、重复次数、开始时间和结束时间不可隐藏。可在上述各项添加筛选条件，对显示结果进行筛选。

3. 点击**确定**。

	事件名称	监听设备	事件等级	重复次数	开始时间	结束时间
1	Samba NDR MS-RPC请求多个远程堆溢出漏洞	eth1		32124	2018-11-27 13:12:36	2018-11-27 15:39:36
2	Samba CVE-2015-0240 Remote Command Exec	eth1		30808	2018-11-27 13:12:47	2018-11-27 15:39:36
3	Microsoft SQL Server xp_showcolv 扩展存储过程远	eth1		6885	2018-11-27 13:12:06	2018-11-27 15:40:29
4	CA BrightStor ARCserve Backup远程缓冲区溢出漏	eth1		5399	2018-11-27 13:13:50	2018-11-27 15:40:37
5	RPC扫描	eth1		4467	2018-11-27 13:12:05	2018-11-27 15:39:33
6	Microsoft PPTP服务程序和客户端远程缓冲区溢出漏洞	eth1		4060	2018-11-27 13:13:09	2018-11-27 15:40:14
7	多家厂商TCP/IP协议栈实现ICMP拒绝服务漏洞	eth1		2898	2018-11-27 13:12:05	2018-11-27 15:40:48
8	Microsoft SQL Server远程拒绝服务漏洞	eth1		2091	2018-11-27 13:12:56	2018-11-27 15:39:42
9	Borland InterBase SVC_attach() Buffer Overflow	eth1		1609	2018-11-27 13:13:17	2018-11-27 15:40:25
10	Borland InterBase ibserver.exe远程栈缓冲区溢出漏	eth1		1552	2018-11-27 13:13:38	2018-11-27 15:40:25

- 双击条目，可以查看该攻击的详细信息。
- 点击**导出**，可下载 Excel 表格到本地电脑。

5.8.连接统计

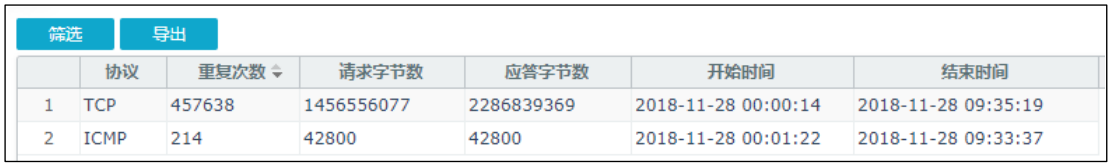
安全管理员可在此查看连接统计情况，统计时间区间支持今天、本周、本月和自定义。同时可选择统计信息的表头显示项。并可对各显示项设置筛选条件，查看符合自定义条件的连接信息。

要查看连接统计，请以安全管理员的身份登录，并执行以下操作：

1. 选择**网络审计>连接统计**。
2. 点击**筛选**，选择显示内容并填写筛选条件。

- 时间范围：缺省情况下，显示今天受攻击情况。可选择**今天**、**本周**、**本月**和**自定义**。选择自定义后，需指定时间区间。
- 统计维度：包括**重复次数**、**收发字节数**、**请求字节数**和**应答字节数**。
- 显示：可选择勾选或者不勾选，在此处选择统计列表的显示项，同时也是筛选依据。包括：协议、监听设备、源 IP、目的 IP 和目的端口。可在上述各项添加筛选条件，对显示结果进行筛选。

3. 点击**确定**。



点击**导出**，可下载 Excel 表格到本地主机。

第6章 报表管理

报表用于统计网络攻击相关的数据并以图表的形式分类显示。本章介绍 NetEye IDS 的报表功能，包括以下内容：

6.1.报表计划任务

安全管理员可以制定具体的报表生成计划，使 NetEye IDS 按照计划在规定的时间自动生成报表。要配置报表生成计划，请以安全管理员身份登录，并执行以下操作：

1. 选择**报表管理>报表计划任务**。
2. 点击**新建**，添加报表生成计划：

a) 设置报表计划名称、报表标题、报表描述信息。

b) 设置报表生成时间，包括每天、每周、每月、立即。可通过点击时间图标前面的下拉框选择生成报表的具体时间点。同时，当选择每周时，可以选择设定具体周几生成报表，如每周一。当选择每月时，可以选择具体哪天生成报表，如每月一号。

c) 当选择“立即”时，设置报表内容覆盖的时间段，包括今天、近 3 天、近 7 天、近 10 天、近 15 天、近 30 天。

d) 点击**确定**。

3. 查看生成的报表计划。

6.2.报表数据

设置完报表生成计划后，NetEye IDS 将根据计划在指定的时间自动生成报表。

要查看生成的报表，请以安全管理员身份登录，并执行以下操作：

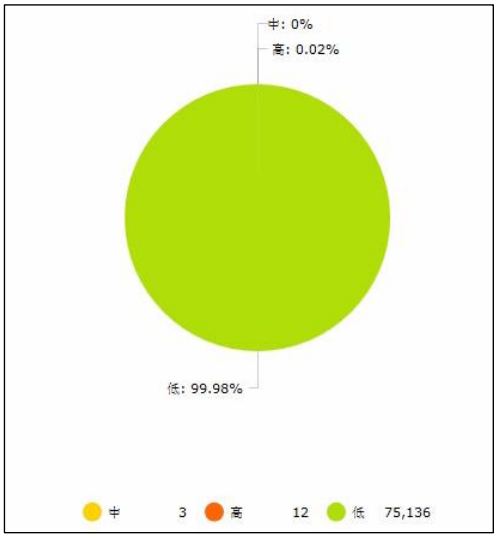
1. 选择**报表管理>报表数据**。
2. 查看生成的报表。

点击 在线查看报表。

点击 下载指定的报表文件到本地，解压缩后可以查看报表内容。

点击 删除指定报表，或勾选多个报表并点击**删除**按钮批量删除报表。

报表参数和样例

参数	**样例**
1. 事件等级发生攻击次数	

2. 事件等级发生最多攻击事件　　包括高、中、低等级事件：

■ 高等级事件

事件名称	发生次数
ADMw0rm ftp 登录企图	9
ADMw0rm ftp 登录企图	3

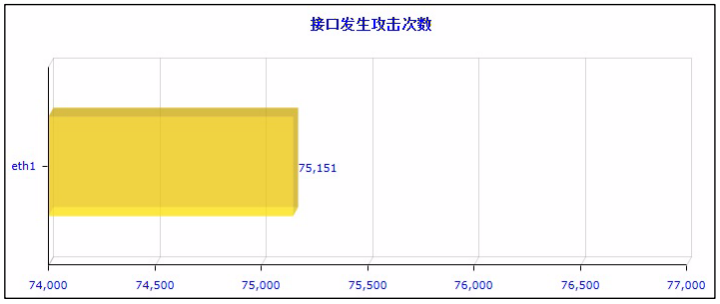
■ 中等级事件

事件名称	发生次数
SCAN UPnP 服务探测	3

■ 低等级事件

事件名称	发生次数
ICMP PING	26064
ICMP 回显应答	26064
ICMP PING Windows	22974
FTP 错误登录	13
FTP 空口令	11

3. 接口发生攻击次数



4. 接口发生最多的攻击事件　　分接口显示：

4.1 eth1

事件名称	发生次数
ICMP PING	26064
ICMP 回显应答	26064
ICMP PING Windows	22974
FTP 错误登录	13
FTP 空口令	11

5. 发生攻击次数最多的事件

事件名称	发生次数
ICMP PING	26064
ICMP 回显应答	26064
ICMP PING Windows	22974
FTP 错误登录	13
FTP 空口令	11

6. 发起攻击次数最多的 IP

源IP地址	发生次数
1.1.1.3	49071
1.1.1.4	26080

7. 攻击次数最多的 IP 发起最多攻击事件

按 IP 分别显示

1.1.1.3

事件名称	发生次
ICMP PING	26064
ICMP PING Windows	22974
FTP 空口令	11
FTP 匿名用户(anonymous)登录	10
ADMw0rm ftp 登录企图	9

8. 被攻击次数最多的 IP

目的IP地址	发生次数
1.1.1.4	49071
1.1.1.3	26077
239.255.255.250	3

9. 被攻击次数最多的 IP 收到最多攻击事件

1.1.1.4

事件名称	发生次
ICMP PING	26064
ICMP PING Windows	22974
FTP 空口令	11
FTP 匿名用户(anonymous)登录	10
ADMw0rm ftp 登录企图	9

10. 发送字节数最多的源 IP

源IP地址	流量
1.1.1.3	238348
1.1.1.4	127258
175.11.11.3	63775

11. 发送字节数最多的目的 IP

目的IP地址	流量
1.1.1.4	154761
255.255.255.255	144730
1.1.1.255	126775
224.0.0.251	2632
239.255.255.250	483

12. 接收字节数最多的源 IP

源IP地址	流量
1.1.1.3	166504
1.1.1.4	0
175.11.11.3	0

13. 接收字节数最多的目的 IP

目的IP地址	流量
1.1.1.4	166504
255.255.255.255	0
1.1.1.255	0
224.0.0.251	0
239.255.255.250	0

14. 发起连接次数最多的 IP

源IP地址	发生次数
1.1.1.3	1083
175.11.11.3	608
1.1.1.4	348

15. 接收连接次数最多的 IP

目的IP地址	发生次数
255.255.255.255	1379
1.1.1.255	347
1.1.1.4	284
224.0.0.251	28
239.255.255.250	1

第7章 系统维护

本章介绍系统维护功能，包括：

提示：“管理用户”和“License管理”功能需要以用户管理员身份登录进行配置，其他功能需要以安全管理员身份登录进行配置。

7.1.管理用户

NetEye IDS 的管理用户分为：用户管理员、安全管理员和审计员。

管理用户权限

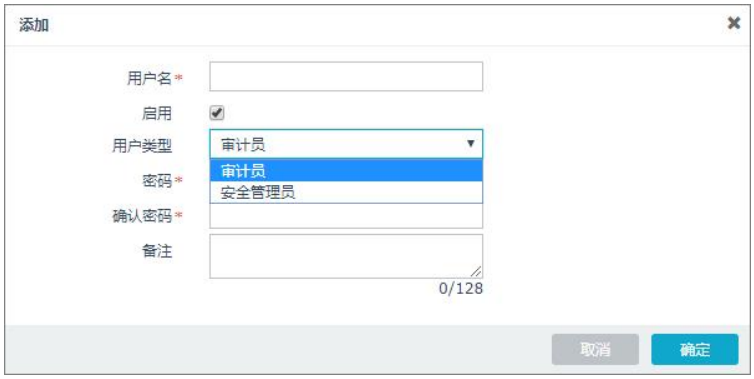
用户角色	用户操作权限
用户管理员	全局唯一，具有以下权限： ■ 查看系统主页信息，包括系统基本信息、资源使用情况、接口状态。 ■ 创建、编辑、删除安全管理员和审计员。 ■ 设置管理员登录时失败次数阈值和超过阈值后系统锁定时间。 ■ License 管理。 ■ 设置其他管理员使用的密码的复杂度。
安全管理员	由用户管理员创建，具有以下权限： ■ 查看系统主页信息，包括系统基本信息、资源使用情况、接口状态、各模块数据库使用情况、实时报警和连接流量统计信息。 ■ 实时监控系统状态，包括实时报警、实时连接状态、实时连接统计、实时数据流量、CPU 使用率和内存使用率。 ■ 查看网络审计信息，包括攻击检测、内容恢复、应用审计、连接审计和网络信息收集。 ■ 进行策略管理，包括引擎接口配置、IP 别名设置、报警配置、入侵检测策略设置、接口配置、过滤配置、内容检测和 NEL 引擎。 ■ 进行系统维护，包括管理接口设置、设备联动配置、系统时间设置、系统管理、报警方式配置、数据备份与恢复、系统升级、访问控制和系统资源告警。 ■ 进行报表管理，包括设置报表生成计划和管理报表数据。 ■ 进行集中管理配置和策略下发。
审计员	由用户管理员创建，具有以下权限： ■ 查看系统主页信息，包括系统基本信息、资源使用情况、接口状态。 ■ 进行日志审计。

系统默认存在一个用户管理员（root/NetEye@1996）、一个安全管理员（admin/NetEye@1996）和一个审计员（audit/NetEye@1996）。root 用户不允许删除。

■ 用户管理员可对安全管理员和审计员进行编辑，如添加、删除等。请以用户管理员登录系统并执行以下操作：

1. 选择**系统维护>管理用户**。

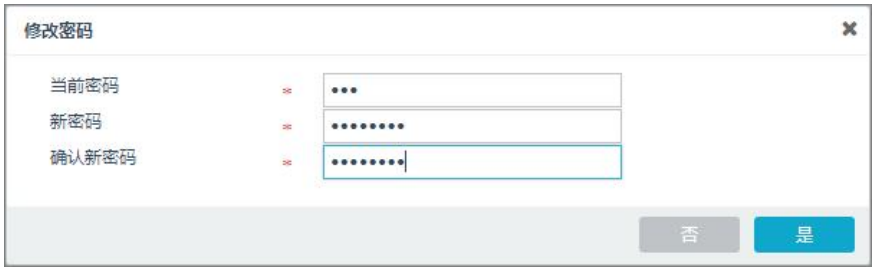
2. 点击**添加**，添加新的安全管理员或审计员。



3. 点击 编辑 root 用户名，点击 编辑用户信息，点击 修改用户密码，点击 删除用户。

提示：如果用户被用户管理员禁用，则此用户不能进行登录认证，只有用户管理员对此用户解禁以后才能继续使用此用户账号登录。

4. 要修改用户管理员 root 的缺省密码，点击页面右上角的，选择，修改密码。



提示：安全管理员和审计员在使用用户名和密码进行初次登录时，为保证安全性，系统会要求更改密码，请根据提示进行。登录成功后，安全管理员和审计员可以通过界面右上角的快捷菜单修改自身密码。

■ 如需对登录密码的强度进行配置，请以用户管理员身份登录系统并进行如下操作：

1. 选择**系统维护>密码策略**。
2. 配置密码的相关要求，包括密码长度限制、大小写限制、数字及特殊符号限制等。

3. 点击**提交**。

■ 如需对登录尝试次数和超过登录阈值后锁定时间以及 Web 超时时间进行配置，请以用户管理员身份登录系统并进行如下操作：

1. 选择**系统维护>登录配置**。
2. 配置锁定时间、尝试次数和 Web 超时时间。缺省情况下，锁定时间为 20 分钟，尝试次数为 5 次，Web 超时时间为 1200 秒。

3. 点击**确定**。

7.2.管理接口

要配置管理接口，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护>管理接口**。
2. 修改管理 IP 地址和网关。

提示：如需解析外部服务器域名（如邮件/Syslog/SNMP Trap日志服务器或FTP备份服务器），则需配置DNS服务器地址。

3. 点击**确定**。

7.3.设备联动配置

NetEye IDS 能够与自有防火墙联动，使防火墙切断被检测出威胁的连接，同时也可根据此条威胁给防火墙添加访问控制策略，在之后的流量中阻断此条威胁中源 IP 地址到目的 IP 地址的连接。要想使用切断连接功能，需要在**策略管理>策略配置>入侵检测策略**中的对应规则处勾选**防火墙联动**。

要想配置设备联动功能，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护>设备联动配置**。
2. 配置要连接的防火墙的网络信息，选择要进行的联动动作。

- **IP 地址/端口**：对端防火墙的管理 IP 地址和端口号。端口号为与防火墙建立 SSH 连接的端口号，缺省为 22。
- **用户名/密码**：对端防火墙的用户名和密码。
- **联动方式**：支持切断连接和加载规则。**切断连接**表示，当连接命中开启防火墙联动功能的规则时，通知防火墙切断该条连接。**加载规则**表示，当连接命中开启防火墙联动功能的规则时，在防火墙上设置一条阻断访问策略，在此后的流量中阻断以该连接的源、目的 IP 地址为基础建立的连接。

3. 点击**提交**。

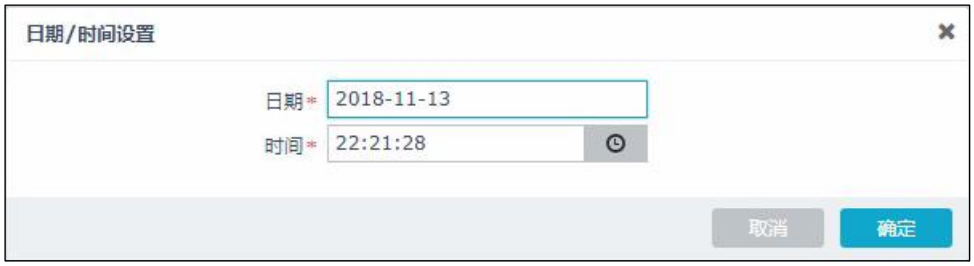
7.4.系统时间

只有系统时间准确，系统才能准确记录系统日志，为管理员提供更加可靠的参考信息。

要配置系统时间，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护>系统时间**。

2. 点击**当前时间**后面的编辑图标 可以修改系统时间。



3. 点击**系统时间同步**后面的编辑图标，可启用时间自动同步。需要设置校时服务器地址、同步方式和校时精度。

- 秘钥 ID：服务器上秘钥的 ID。
- 预共享密钥：服务器上配置的秘钥，与秘钥 ID 成对出现。

4. 点击**确定**。

提示：设置新的系统时间后，重叠时间内的数据将被删除。也就是说，如果将系统时间往前修改，重叠时间段内新产生的数据将覆盖之前产生的数据。

7.5.系统管理

系统管理中提供三个按钮，分别为**重启系统**按钮、**关闭系统**按钮和**重置系统**按钮。

请使用安全管理员账号登录系统，并执行以下步骤：

1. 选择**系统维护>系统管理**。

2. 点击所需按钮。
3. 点击**确定**。

7.6.报警方式配置

为了实时了解网络安全状态，管理员一般都会配置日志报警。要使用日志报警功能，首先需要正确配置日志服务器地址，然后配置报警策略。NetEye IDS 支持三种日志报警方式：邮件、Syslog 和 SNMP Trap。

提示：在对报警方式进行配置的同时，还需在策略管理>策略配置中对相应策略的相应事件的报警方式进行勾选，相应报警才能够产生。

7.6.1. 邮件报警配置

要配置邮件报警服务器地址，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护>报警方式配置> 邮件报警**。

a) 启用邮件报警功能，并设置报警邮件发送间隔。

a) 设置 SMTP 服务器地址和端口号。如果该服务器启用身份认证，还需要设置用户名和密码。

b) 设置报警邮件的发送者、标题和接收者。多个接收者地址之间用“;”隔开。

2. 点击**确定**。

7.6.2. Syslog 报警配置

要配置 Syslog 报警服务器地址，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护>报警方式配置> Syslog 报警**。

设备支持标准格式的 syslog 日志，同时也支持简洁模式。

简洁模式格式如下：

事件描述<空格>源 IP 地址<空格>源端口<空格>目的 IP 地址<空格>目的端口

2. 启用 Syslog 报警功能，点击**添加**，并设置 Syslog 服务器地址。
3. 点击**确定**。

7.6.3. SNMP Trap 报警配置

对于网络中原本就使用网络管理软件的用户来说，如果 NetEye IDS 产生的报警消息可以被他们的网管软件所接收，那就意味着其现有网络资源可以得到最大限度的利用，而且可以实现对包括入侵在内的各种网络异常现象的统一管理。NetEye IDS 可以通过 SNMP Trap 消息，将报警事件发送到网管平台，实现与各类网管平台的集成。

要配置 SNMP Trap 报警服务器地址，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护>报警方式配置> SNMP Trap 报警**。

2. 启用 SNMP Trap 报警功能，设置 SNMP 服务器地址，并选择使用的 SNMP 传输协议版本，包括 SNMPv1 和 SNMPv2c 两种。
3. 点击**确定**。

7.7.备份/恢复

本节介绍如何备份及恢复数据，系统支持本地备份和备份到 FTP 服务器。

7.7.1. FTP 配置

NetEye IDS 支持通过 FTP 自动进行系统备份。要使用该功能，需要先配置 FTP 服务器。只有正确配置 FTP 服务器并启用 FTP 自动备份功能，数据才可以自动备份到相应 FTP 服务器的指定目录。

要配置 FTP 备份，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护> 备份/恢复> FTP 配置**。
2. 启用 FTP 备份，并设置 FTP 服务器地址和端口、用户名和密码以及备份路径。

默认备份路径为当前用户的起始目录；用户可设置自己的备份目录，若目录不存在，则创建相应的目录。

设置完毕后，可点击**测试 FTP 服务器**，测试 FTP 服务器是否连通。在测试连通性之前需在 FTP 服务器上开启服务器相应的读写权限。

3. 在 **FTP 自动备份设置**区域启用自动备份，设置备份的数据库类型和每天执行自动备份的时间。

提示：自动备份功能会检查备份目录，进行增量备份，对已备份的数据不再执行备份。

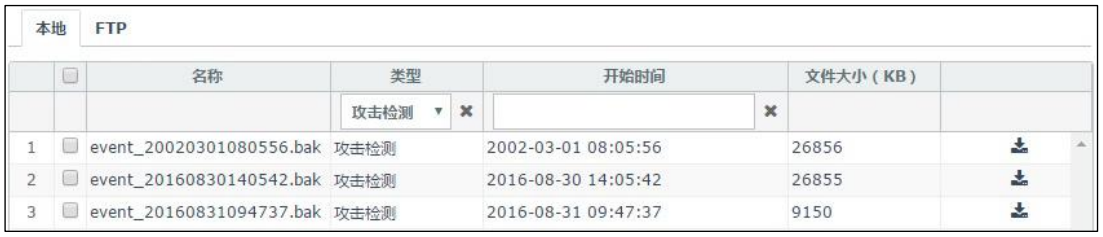
4. 点击**确定**。

7.7.2. 数据管理

NetEye IDS 支持系统备份和恢复功能，可采取两种方式进行备份：下载至管理主机或备份到 FTP 服务器。

要使用数据管理功能，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护>备份/恢复>数据管理**。
2. 在**本地**页面，可以查看 NetEye IDS 的所有备份文件（系统自动生成）。



点击 下载备份文件到当前管理主机。

安全管理员可以通过**类型**下拉框和**开始时间**文本框筛选备份文件。备份文件类型包括**攻击检测**、**连接审计**、**应用审计和内容恢复**。点击**开始时间**文本框，可以通过时间控件选择备份数据的起始记录时间。

3. 点击 **FTP** 选项卡，打开 FTP 备份恢复页面，可以查看 NetEye IDS 本地和远程 FTP 服务器上的所有备份文件。

安全管理员可以通过**类型**下拉框和**开始时间**文本框筛选备份文件。**开始时间**即备份文件中第一条数据记录的开始时间。

本地列的绿色图标表示备份文件在 NetEye IDS 本地，**FTP** 列的绿色图标表示备份文件在 FTP 服务器上。

勾选本地备份文件复选框并点击**备份**按钮可将文件备份到到 FTP 服务器，同时灰色图标变为绿色图标。

点击，查看备份文件基本信息。点击**确定**，将 FTP 上的备份文件数据恢复到 NetEye IDS，可以在**备份数据浏览**页面查看。

7.7.3. 备份数据浏览

NetEye IDS 支持安全管理员导入并查看备份数据。

要查看或导入备份数据，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护>备份/恢复>备份数据浏览**。
2. 查看恢复的备份数据。双击条目可以查看详细信息。

	传输协议	连接状态	监听设备	源 IP	目的 IP	目的端口	连接次数	请求字节数	应答字节数	时间
	All									
1	TCP	TCP_CLOSE	eth0	192.168.130.249	192.168.130.11	80	1	118	285	2016-08-26 18:35:06
2	TCP	TCP_CLOSE	eth1	9.1.1.1	9.1.1.2	21	93	69378	20181	2016-08-26 18:35:05
3	UDP	UDP	eth0	1.1.1.3	255.255.255.255	164	1	105	0	2016-08-26 18:34:53
4	ICMP	ICMP	eth1	1.1.1.1	192.168.50.1	0	1	60	0	2016-08-26 18:34:53
5	UDP	UDP	eth0	172.31.9.254	255.255.255.255	164	1	105	0	2016-08-26 18:34:52
6	UDP	UDP	eth0	10.1.3.156	10.1.7.255	138	1	229	0	2016-08-26 18:34:52
7	UDP	UDP	eth0	192.168.130.101	192.168.130.255	138	1	232	0	2016-08-26 18:34:47
8	UDP	UDP	eth0	192.168.100.120	255.255.255.255	164	1	105	0	2016-08-26 18:34:45
9	UDP	UDP	eth0	192.168.130.252	224.0.0.252	5355	2	212	0	2016-08-26 18:34:43
10	UDP	UDP	eth0	10.1.2.139	239.255.255.250	1900	1	912	0	2016-08-26 18:34:38
11	TCP	TCP_CLOSE	eth1	9.1.1.1	9.1.1.2	21	92	68632	19964	2016-08-26 18:34:35
12	UDP	UDP	eth0	10.1.3.91	10.1.7.255	138	1	229	0	2016-08-26 18:34:32
13	UDP	UDP	eth0	192.168.130.120	192.168.130.255	137	1	78	0	2016-08-26 18:34:31
14	UDP	UDP	eth0	10.1.3.61	224.0.0.251	5353	1	348	0	2016-08-26 18:34:29
15	UDP	UDP	eth0	10.1.6.168	10.1.7.255	161	2	18796	0	2016-08-26 18:34:28
16	UDP	UDP	eth0	10.1.3.61	224.0.0.252	5355	2	226	0	2016-08-26 18:34:26
17	UDP	UDP	eth1	1.1.1.1	192.168.50.2	161	1	128	0	2016-08-26 18:34:26
18	UDP	UDP	eth0	10.1.2.38	10.1.7.255	138	1	229	0	2016-08-26 18:34:20
19	UDP	UDP	eth0	10.1.3.44	10.1.7.255	1947	1	68	0	2016-08-26 18:34:13
20	UDP	UDP	eth0	10.1.3.44	255.255.255.255	1947	1	68	0	2016-08-26 18:34:09
21	TCP	TCP_CLOSE	eth0	192.168.130.249	192.168.130.11	80	1	118	285	2016-08-26 18:34:06
22	TCP	TCP_CLOSE	eth0	10.1.4.59	10.1.6.90	443	2	18348	17405	2016-08-26 18:34:05
23	TCP	TCP_CLOSE	eth1	9.1.1.1	9.1.1.2	21	93	69378	20181	2016-08-26 18:34:05

3. 点击**导入**，可以导入新的备份文件进行查看。

7.8.数据库维护

本节介绍如何对数据库空间进行管理，包括：

7.8.1. 数据库空间管理

此功能帮助您更好地管理数据库空间。系统会自动将磁盘分配给攻击检测、内容检测、应用审计和连接审计四个功能进行使用。在界面中能看到有四个页签，每个页签有数据库信息和数据库删除两部分构成。数据库信息包括：已用空间、可用空间和总计空间。用户可以从此看出磁盘空间的使用情况。在数据库删除栏由已用空间和删除数据按钮组成。已用空间能够看出磁盘空间整体使用情况。**按条件删除**按钮能够根据条件删除相应数据，操作步骤如下：

1. 选择**系统维护>数据库维护>数据库空间管理**。

2. 点击**按条件删除**，根据需要进行配置。

3. 点击**确定**。

7.8.2. 数据库设置

此功能用于设置磁盘记录满后系统所做的动作及数据库数据的全部删除。

1. 选择**系统维护>数据库维护>数据库设置**。
2. 在界面中进行所需配置。
   - 在记录方式中选择**覆盖记录**或**停止记录**，并点击**确定**。

   - 点击**删除**，并点击**确定**，删除所有数据。

7.9.系统升级

7.9.1. 规则库升级

东软有专门的网络安全攻防团队不断的更新攻击检测规则，为了不断增强 NetEye IDS 的攻击检测能力，建议安全管理员定期升级入侵检测规则库。

要升级规则库，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护>系统升级**。
2. 在**系统信息**区域查看系统当前型号和软件版本信息。

3. 点击**上载规则库升级包**，手动上传规则升级文件。确认后，系统升级并断开当前连接，管理员需要重新登录。

4. 升级成功后，可在**升级信息**区域查看系统升级历史信息。

7.9.2. 系统升级

系统升级通常包括对系统缺陷的修复或对系统功能、性能的增强。

要进行系统升级，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护>系统升级**。

2. 点击**上载系统升级包**，手动上传系统升级文件。确认后，系统升级并断开当前连接，管理员需要重新登录。
3. 升级成功后，可在**升级信息**区域查看系统升级历史信息。

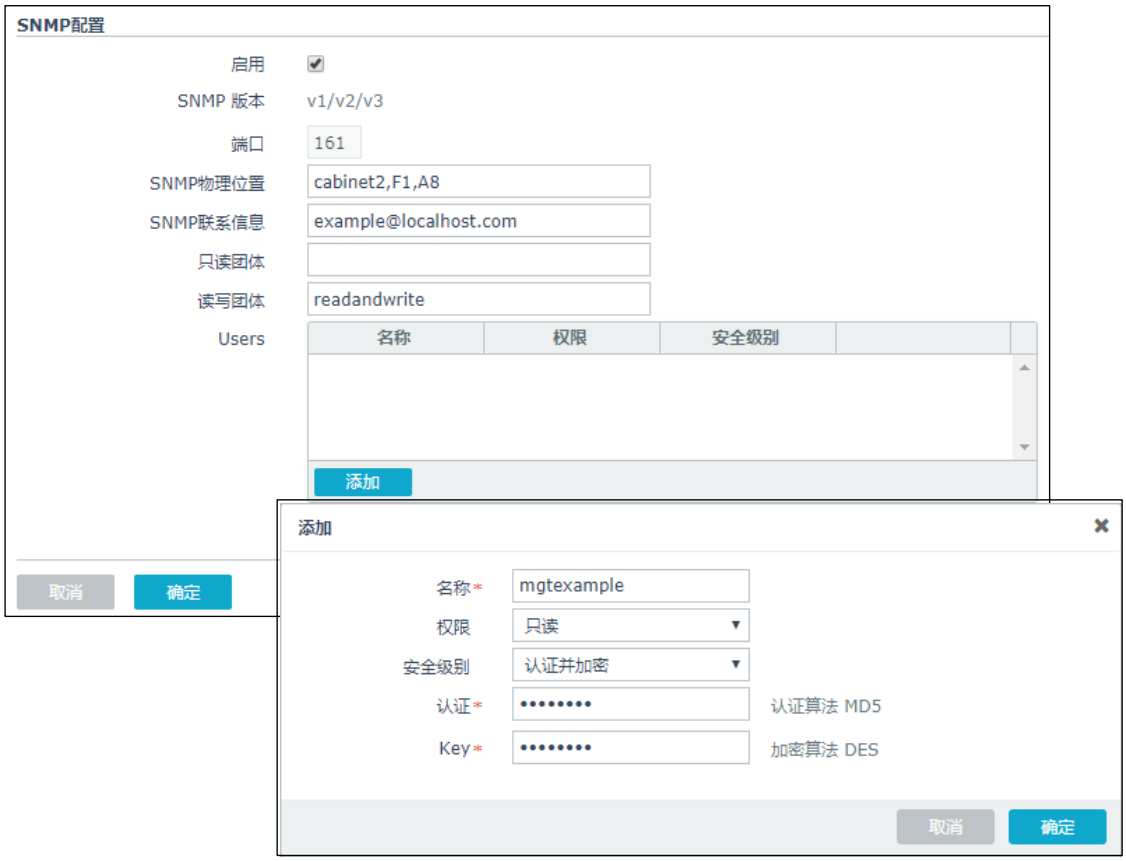
7.10.SNMP 配置

NetEye IDS 支持通过 SNMP 被网络管理站管理。

支持的 SNMP 版本有 SNMPv1、SNMPv2 和 SNMPv3。

要进行 SNMP 配置，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护> SNMP 配置**。
2. 勾选启用 SNMP 配置，根据使用的 SNMP 版本配置所需信息。



- **SNMP 物理位置**：描述设备物理位置的字符串。
- **SNMP 联系信息**：管理员的联系信息。
- **只读团体**：管理站读取设备信息时进行身份识别的字符串。
- **读写团体**：管理站读取或修改设备信息时进行身份识别的字符串。
- **Users**：当时用 SNMPv3 时需要配置 SNMP 用户，所需配置信息如下：
  - **名称**：SNMPv3 用户的名称。
  - **权限**：包括**只读**和**读写**。**只读**表示，只可以查询设备的状态信息。**读写**表示，既可以查询设备的状态信息，又可以修改设备的部分配置信息。可修改的配置信息包括团体字符串、物理位置字符串和联系信息字符串。

- **安全级别**：管理站与设备通信的安全级别。包括认证并加密、认证但不加密和不认证不加密。选择不认证不加密时不需要配置认证和 Key。
- **认证**：用于确认身份的字符串。
- **Key**：用于信息加密的字符串。

3. 点击**确定**。

7.11.访问控制

本地访问控制功能主要用于限定访问 NetEye IDS 的 IP 范围。通过配置访问控制，管理员可以只允许特定的主机对 NetEye IDS 进行访问。

要配置访问控制，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护>访问控制**。
2. 启用本地访问控制（包括 https 和 ping），添加被允许的 IP 地址或子网：

3. 点击**确定**。
4. 点击 **SSH 访问控制**，根据需要启用或禁用 SSH 访问控制。

7.12.系统资源告警

如果配置系统资源告警，一旦系统资源使用率超过指定的阈值，系统可以在界面右上方的快捷菜单处给与提示。

要配置系统资源告警功能，请以安全管理员身份登录，并执行以下操作：

1. 选择**系统维护>系统资源告警**。

2. 设置 CPU、内存和磁盘资源使用上限，以及超过上限时是否报警。勾选**忽略**表示即使达到阈值也不进行报警。
3. 点击**确定**。

7.13.License 管理

NetEye IDS 未上载 License 时，各缺省管理用户的权限如下：

缺省用户	权限
用户管理员 root	仅可以查看主页信息、管理 License，不能配置管理用户。
安全管理员 admin	仅可以查看主页信息、修改管理接口、升级规则库、升级系统，不能进行其他系统操作。
审计员 audit	仅可以查看主页信息，不能查看系统日志。

要想使用 NetEye IDS 的全部功能，需要上载有效的 License。NetEye IDS 出厂已经上载 License。如果在使用 NetEye IDS 的期间改变了系统硬件配置，包括改变网卡等，则需要生成 License 请求文件，然后提交给 NetEye IDS 技术支持工程师，重新制作 License 文件。

要管理 License，请以用户管理员身份登录，进行如下操作：

1. 选择**系统维护> License 管理**。
2. 点击**生成 License 请求**，下载生成的请求文件，发送给厂商制作 License。
3. 获得 License 后，点击**导入**，上载 License 文件。

第8章 集控中心

本章介绍 NetEye IDS 的集中管理功能，内容包括：

8.1.集中管理

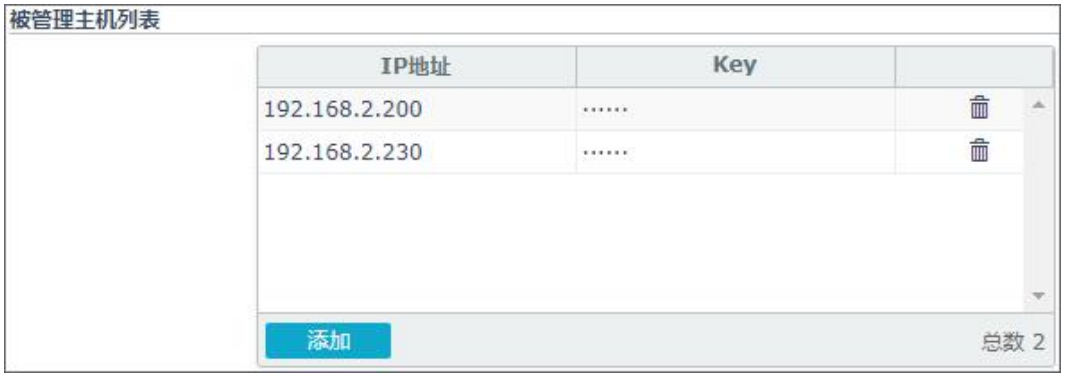
NetEye IDS 提供集中管理功能，支持多级管理，一个 NetEye IDS 系统可以同时管理多个被管理 NetEye IDS 系统。

要配置集中管理功能，请以安全管理员身份登录，并执行以下操作：

1. 选择**集控中心>集中管理**。
2. 启用多级管理，设置授权密钥。

授权密钥即当前 NetEye IDS 被上一级 NetEye IDS 管理时使用的密钥，要求管理端和被管理端必须一致。

3. 添加被管理 NetEye IDS 的 IP 地址和管理密钥。



- **IP 地址**：即被管理端的管理 IP 地址。
- **Key**：即被管理端上设置的集中管理授权密钥。

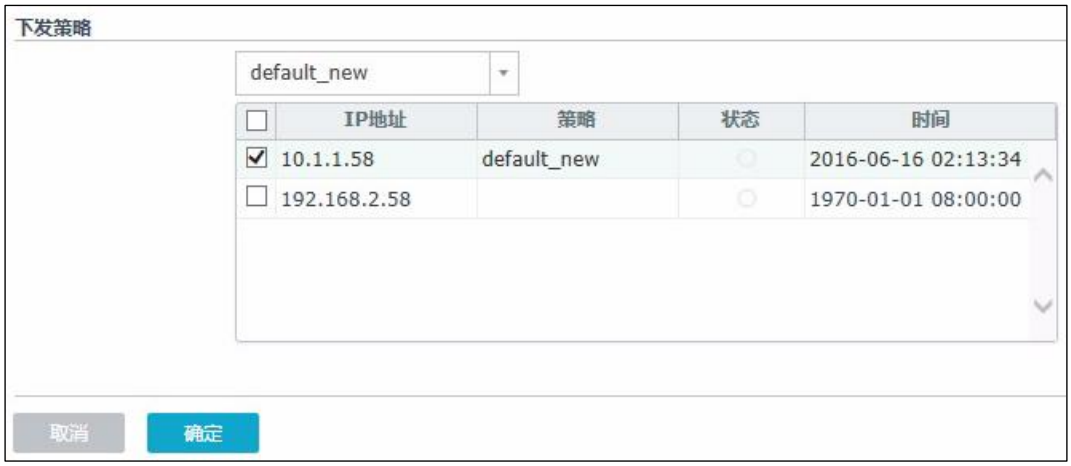
4. 点击**确定**。

8.2.下发策略

开启集中管理功能的 NetEye IDS 系统可以向被管理系统下发策略。

要设置下发策略功能，请以安全管理员身份登录，并执行以下操作：

1. 选择**集控中心>下发策略**。
2. 从下拉框中选择要下发的本地策略，在列表中选择要向其下发策略的被管理系统，点击**确定**。



3. 可登录被管理端，选择**策略管理>策略配置>入侵检测策略**，查看策略是否下发成功。

第9章 日志审计

本章介绍 NetEye IDS 的日志审计功能。

NetEye IDS 记录两类日志：网络安全日志和系统日志。网络安全日志记录网络中发生的攻击事件，系统日志记录系统本身相关的一些配置和管理事件。

要查看网络日志信息，请以安全管理员身份登录，并查看实时监控和网络审计信息。

要查看系统日志信息，请以审计员身份登录，并执行以下操作：

1. 选择**日志审计>系统日志**。
2. 查看系统日志信息。

	事件类型	事件内容	用户	客户端IP	发生次数	发生时间
	全部					
1	信息	用户登录成功	audit	10.1.4.149	1	2016-09-01 14:39:04
2	信息	用户登录成功	admin	10.1.4.149	1	2016-09-01 14:20:15
3	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:17:14
4	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:17:08
5	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:17:01
6	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:17:00
7	信息	用户登录成功	audit	10.1.4.149	1	2016-09-01 14:12:20
8	警告	用户登录失败	N/A	10.1.4.149	1	2016-09-01 14:12:14
9	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:12:12
10	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:12:10
11	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:12:07
12	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:12:04
13	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:05:31
14	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:05:28
15	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:05:26
16	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:05:09
17	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:05:02
18	信息	获取FTP服务器文件列表成功	admin	10.1.4.59	1	2016-09-01 14:05:01
19	信息	继承策略成功	admin	10.1.4.149	1	2016-09-01 11:58:44
20	信息	添加报表计划成功	admin	10.1.4.149	1	2016-09-01 11:39:48
21	信息	用户登录成功	admin	10.1.4.149	1	2016-09-01 09:38:08
22	信息	备份到FTP服务成功	admin	10.1.4.149	1	2016-08-31 17:49:17
23	信息	获取FTP服务器文件列表成功	admin	10.1.4.149	1	2016-08-31 17:47:25

第 1 页

可通过事件类型、事件内容、操作用户、客户端 IP 和操作发生时间筛选查看的系统日志，点击右侧的 ✖ 可以清除筛选条件。

每页最多显示 100 条，超过 100 条分页显示，通过页码前后的箭头可以翻页查看。

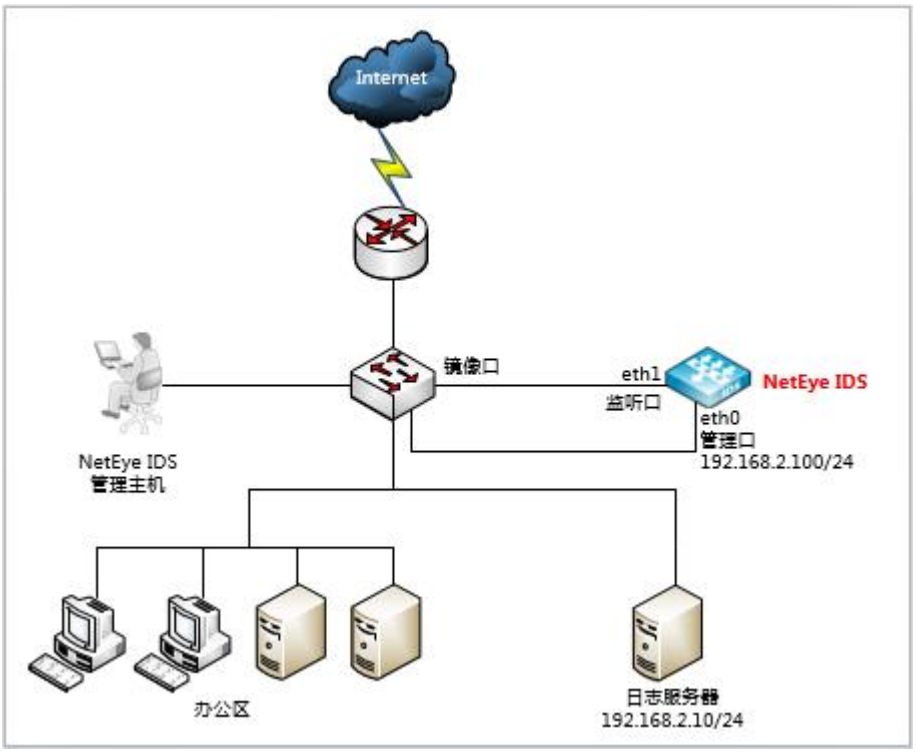
系统日志记录的事件分为三类：信息、警告、错误。信息是对正常操作的记录；警告是对一般性错误操作的记录；错误是对影响系统正常运行的操作的记录。

第10章 典型部署示例

本章给出 NetEye IDS 的典型部署示例，包含以下内容：

10.1.典型部署

NetEye IDS 主要以旁路模式部署在网络中，通常使用单一接口独立监听，网络拓扑如下所示：



10.2.配置准备

1. 规划网络：
   - eth1 为监听接口，连接到核心交换机的镜像接口；
   - eth0 为管理接口，管理 IP 为 192.168.2.100/24，网关为 192.168.2.1；
   - 管理主机需要增加 192.168.2.0/24 网段的 IP 地址，与 NetEye IDS 管理口通信；
   - 内网日志服务器的 IP 地址为 192.168.2.10/24，网关为 192.168.2.1。
2. 配置核心交换机的镜像接口，将要监控的网络流量拷贝到 NetEye IDS。

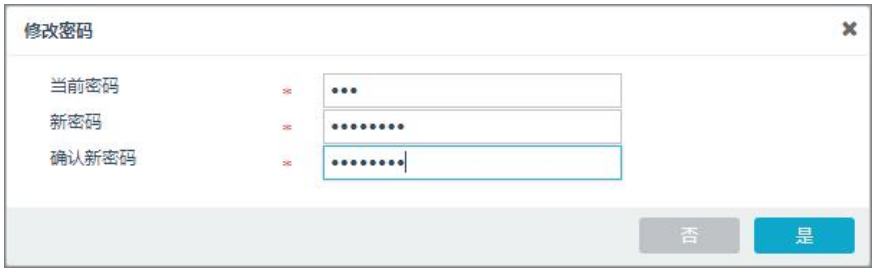
10.3.配置步骤

10.3.1. 修改密码

系统默认存在一个用户管理员（root/NetEye@1996）、一个安全管理员（admin/NetEye@1996）、一个审计员（audit/NetEye@1996）。建议先以 root 用户身份登录并修改缺省密码，然后以 admin 用户身份登录并修改密码，之后进行相关配置。

1. 以 root 用户身份登录，选择**系统维护>管理用户**。

2. 点击页面右上角的，选择，修改 root 用户缺省密码，点击**是**。



3. 点击页面右上角的，选择，退出系统，并以安全管理员 admin 身份登录系统。
4. 根据系统提示修改登录密码。

5. 密码修改完成后，使用新密码重新登录。

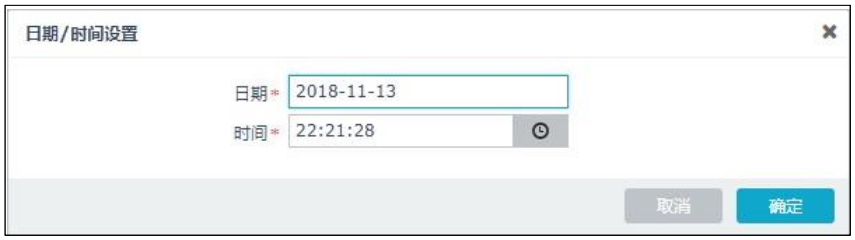
10.3.2. 修改管理接口/IP

1. 选择**系统维护>管理接口**。
2. 修改管理 IP 地址和网关。

3. 点击**确定**。

10.3.3. 更新系统时间

1. 选择**系统维护>系统时间**。
2. 点击**当前时间**后面的编辑图标，修改系统时间。



3. 点击**确定**。

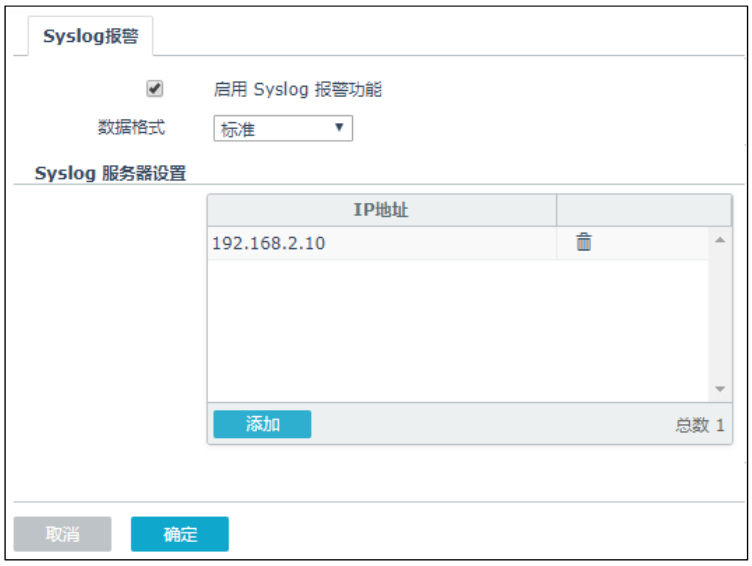
4. 点击系统时间同步后面的编辑图标，配置系统与 NTP 服务器进行时间同步。

5. 点击**确定**。

10.3.4. 配置报警服务器地址

为了实时了解网络安全状态，管理员一般都会配置日志报警。

1. 选择**系统维护>报警方式配置> Syslog 报警**。



2. 启用 Syslog 报警功能，并设置 Syslog 服务器地址。

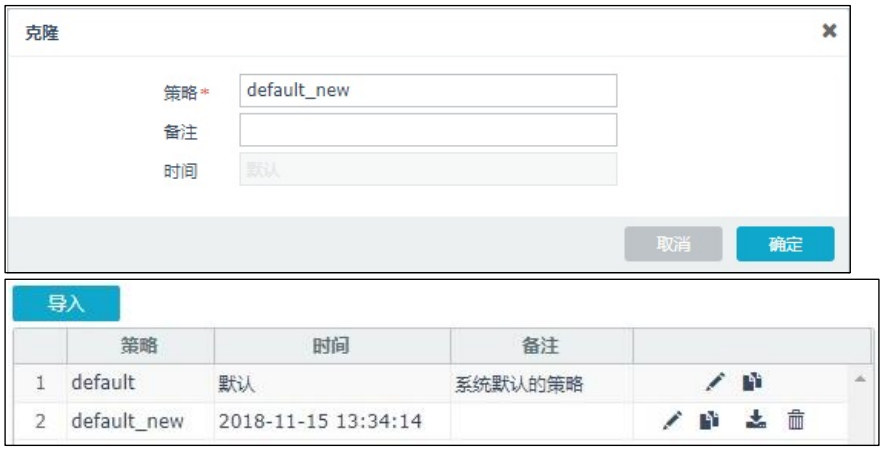
3. 点击**确定**。

10.3.5. 配置入侵检测策略

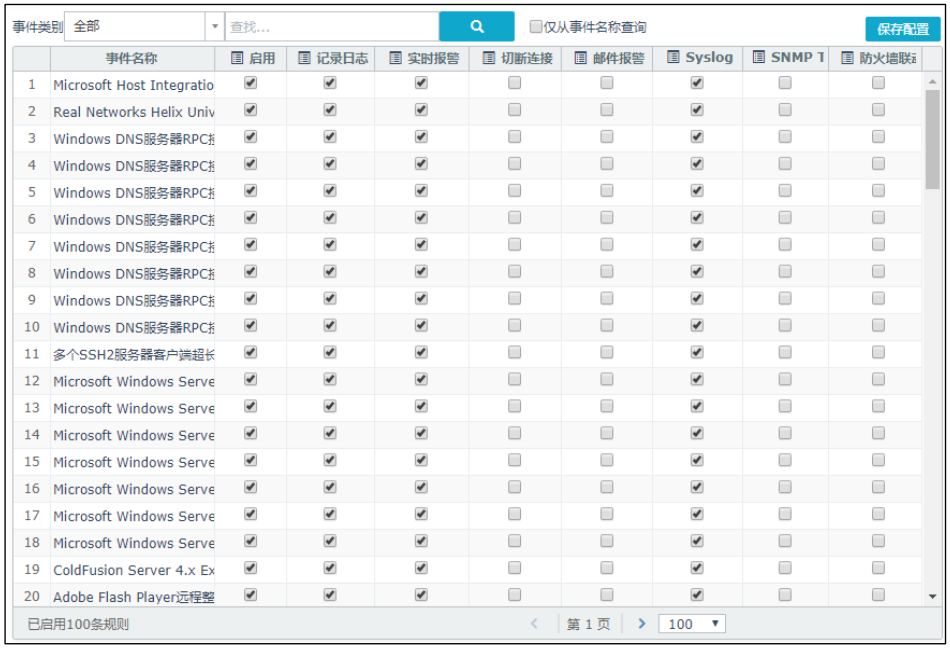
配置监听接口之前，需配置入侵检测策略，即指定要检测的攻击事件。

1. 选择**策略管理>策略配置>入侵检测策略**。

2. 点击缺省策略对应的 图标，设置克隆策略的名称和备注信息。



3. 点击 ，编辑克隆策略的设置，根据需要启用或禁用入侵检测事件规则。



4. 编辑完成后，点击右上方的**保存配置**按钮。

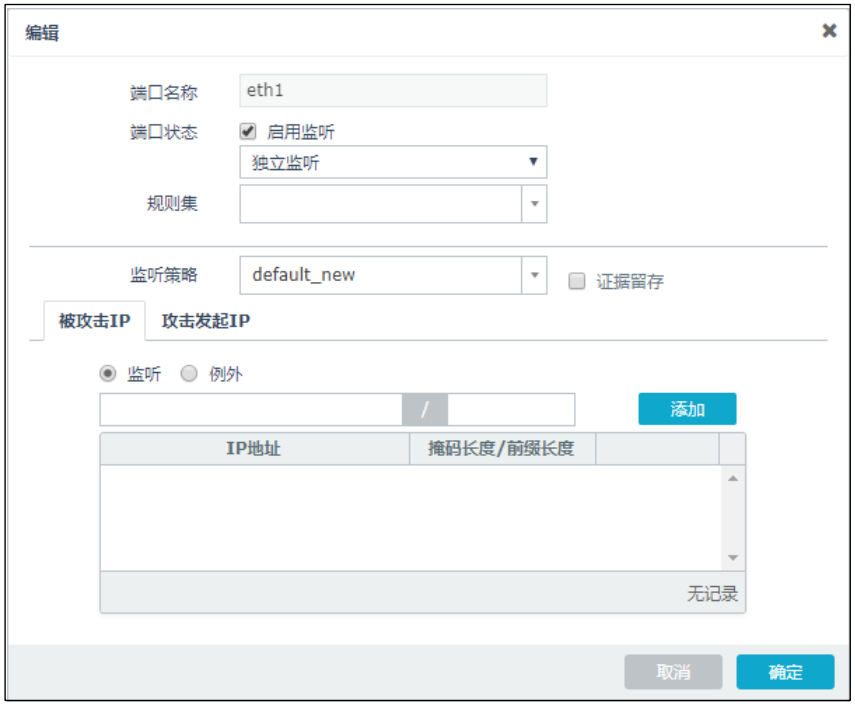
10.3.6. 配置引擎开关及监听接口

在此处配置监听接口并在监听接口上指定启用的入侵检测策略。

1. 选择**策略管理>引擎接口配置**。
2. 开启引擎开关。

3. 选择**使用 eth0 切断**，点击**确定**。

4. 点击接口，设置接口监听状态、监听策略和监听网络。



5. 点击**确定**。

10.4.查看结果

10.4.1. 查看监控信息

完成检测策略和监听接口的配置以后，即可开始监控网络运行状态，包括查看实时报警、实时连接状态和实时数据流量。

要查看网络监控信息，请以安全管理员身份登录，并执行以下操作：

1. 点击主界面右上角的实时报警快捷菜单，或者选择**实时监控>实时报警**，查看最新发生的攻击事件。

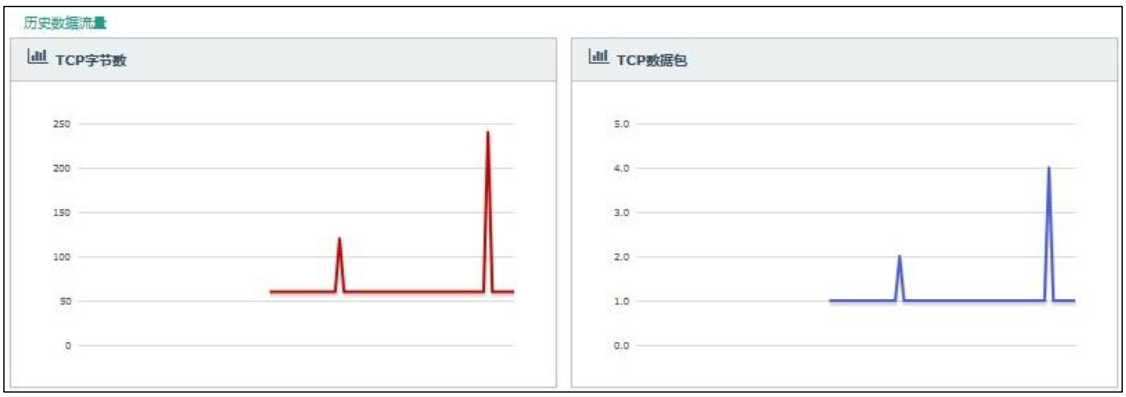
	事件名称	事件等级	重复次数	监听设备	协议	源IP地址	目的IP地址	源端口	目的端口	时间
1	Microsoft SQL Server xp_showcolv 扩展存储过		2	eth1	TCP	10.0.3.91	10.0.3.177	3743	1433	2018-11-27 15:17:33
2	Microsoft SQL Agent Jobs Privilege Elevation		2	eth1	TCP	10.0.3.91	10.0.3.177	3743	1433	2018-11-27 15:17:33
3	HP Network Node Manager I PMD Buffer Over		1	eth1	UDP	10.0.3.46	10.0.3.88	54955	7426	2018-11-27 15:17:15
4	SAP-DB/MaxDB WebDBM 远程缓冲区溢出漏洞		1	eth1	TCP	188.1.5.237	189.1.30.24	20438	9999	2018-11-27 15:17:15
5	University of Washington imap overflow		1	eth1	TCP	10.0.3.113	10.0.3.125	8301	143	2018-11-27 15:17:15
6	University of Washington imap overflow		1	eth1	TCP	10.0.3.113	10.0.3.125	8187	143	2018-11-27 15:17:15
7	University of Washington imap overflow		1	eth1	TCP	172.22.5.218	172.22.5.166	40770	143	2018-11-27 15:17:14
8	Sophos病毒库Visio扫描远程堆溢出漏洞		1	eth1	TCP	10.0.3.9	192.168.234.13	14302	1177	2018-11-27 15:17:14
9	Sophos病毒库Visio扫描远程堆溢出漏洞		1	eth1	TCP	10.0.3.9	192.168.234.13	46026	1114	2018-11-27 15:17:14
10	Microsoft IE URLMON.DLL COM对象实例化无效		2	eth1	TCP	1.255.25.111	1.1.138.184	80	45108	2018-11-27 15:17:13
11	GoodTech SMTP Server RCPT TO多个远程溢出		1	eth1	TCP	188.1.205.13	189.1.21.136	30271	25	2018-11-27 15:17:13
12	GoodTech SMTP Server RCPT TO多个远程溢出		1	eth1	TCP	188.1.246.108	189.1.227.127	35145	25	2018-11-27 15:17:13
13	Phase Zero Trojan Client Command		1	eth1	TCP	1.2.115.227	1.1.231.197	555	52712	2018-11-27 15:17:13
14	Phase Zero Trojan Client Command		1	eth1	TCP	1.2.89.49	1.1.231.40	555	23035	2018-11-27 15:17:13
15	网络神偷 11.1 版		1	eth1	UDP	10.0.0.186	10.0.0.201	3174	2018	2018-11-27 15:17:12
16	Microsoft Windows即插即用功能远程缓冲区溢出		6	eth1	TCP	1.229.96.51	1.255.7.20	2772	139	2018-11-27 15:17:10
17	Microsoft Windows 2000 DCOM RPC接口拒绝服		4	eth1	TCP	10.2.8.149	10.2.1.60	2564	135	2018-11-27 15:17:10
18	RPC扫描		24	eth1	TCP	10.2.8.149	10.2.1.60	2564	135	2018-11-27 15:17:10
19	Microsoft Windows 2000 DCOM RPC接口拒绝服		4	eth1	TCP	10.2.8.149	10.2.1.60	2562	135	2018-11-27 15:17:10
20	RPC扫描		24	eth1	TCP	10.2.8.149	10.2.1.60	2562	135	2018-11-27 15:17:10
21	Microsoft SQL Server xp_showcolv 扩展存储过		8	eth1	TCP	10.2.8.149	10.2.1.60	1028	1433	2018-11-27 15:17:10

2. 选择**实时监控>实时连接状态**，查看实时的网络连接状态。

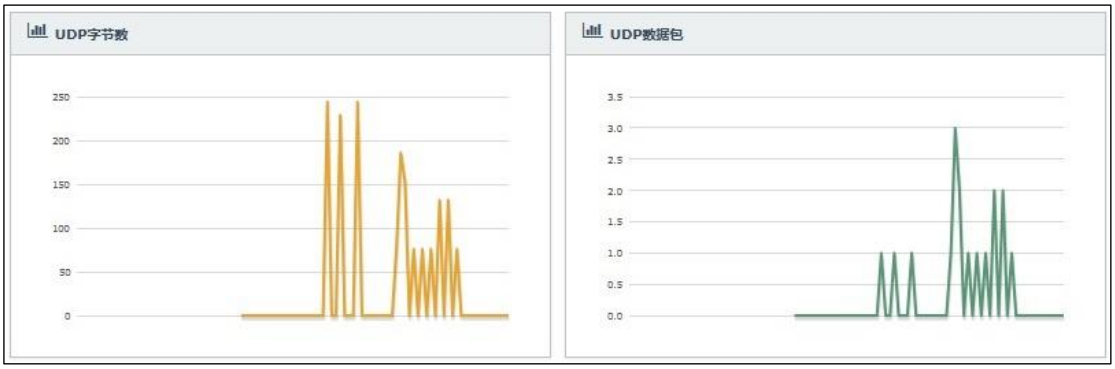
协议	连接状态	监听设备	源 IP	目的 IP	源端口	目的端口	请求字节数	应答字节数	时间	空闲时间（秒
	All									
ICMP	ICMP	eth1	192.168.10.230	192.168.10.231	0	0	440340	440340	2018-11-15 18:48:0	3
	ICMP	eth1	fe80::b023:d41f:1	fe80::20c:29ff:fea	0	0	1174400	1174400	2018-11-15 18:48:2	6
ICMP	ICMP	eth1	10.9.227.223	10.9.227.200	0	0	1321200	1321200	2018-11-15 18:48:2	6
UDP	UDP	eth1	10.240.160.166	224.0.0.253	63739	3544	499188	0	2018-11-15 18:48:2	0
UDP	UDP	eth1	192.168.1.0	192.168.1.1	60000	2140	4404000	14012060	2018-11-15 18:48:1	2
UDP	UDP	eth1	192.168.1.0	192.168.1.1	60000	3150	2745160	0	2018-11-15 18:48:1	2
UDP	UDP	eth1	189.18.53.140	192.168.13.211	61128	8508	178158	158799	2018-11-16 05:04:1	3
UDP	UDP	eth1	192.168.13.211	88.22.197.126	8508	6882	47988	54096	2018-11-16 07:46:4	3
UDP	UDP	eth1	192.168.13.211	62.94.187.134	8508	20731	48504	127792	2018-11-16 07:46:4	3
UDP	UDP	eth1	192.168.13.211	87.120.15.33	8508	8166	48246	130020	2018-11-16 07:46:4	3
UDP	UDP	eth1	192.168.13.211	77.239.234.203	8508	62847	48246	133566	2018-11-16 07:46:4	3
UDP	UDP	eth1	99.246.161.137	192.168.13.211	63125	8508	425370	158283	2018-11-16 05:04:1	3
UDP	UDP	eth1	192.168.13.211	123.212.119.77	8508	38257	47988	140658	2018-11-16 07:46:4	3
UDP	UDP	eth1	71.192.58.119	192.168.13.211	27729	8508	437649	158670	2018-11-16 05:04:1	3
UDP	UDP	eth1	192.168.13.211	71.198.209.184	8508	10780	47988	130350	2018-11-16 07:46:4	3
UDP	UDP	eth1	192.168.13.211	85.138.200.146	8508	24905	50955	0	2018-11-16 07:46:4	3
UDP	UDP	eth1	192.168.13.211	24.166.90.149	8508	20091	47859	130680	2018-11-16 07:46:4	3
UDP	UDP	eth1	70.140.24.160	192.168.13.211	15425	8508	199584	158154	2018-11-16 05:04:1	3

3. 选择**实时监控>实时数据流量**，查看实时的网络流量信息，包括：

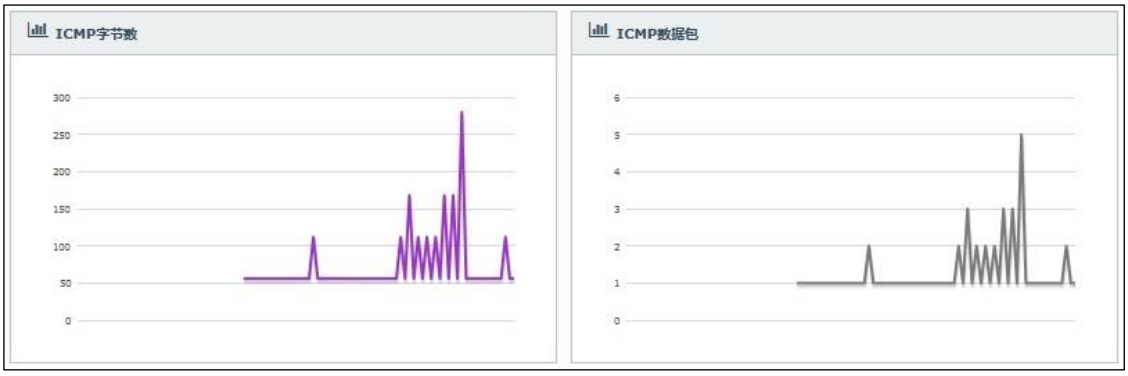
- TCP 字节数和数据包数



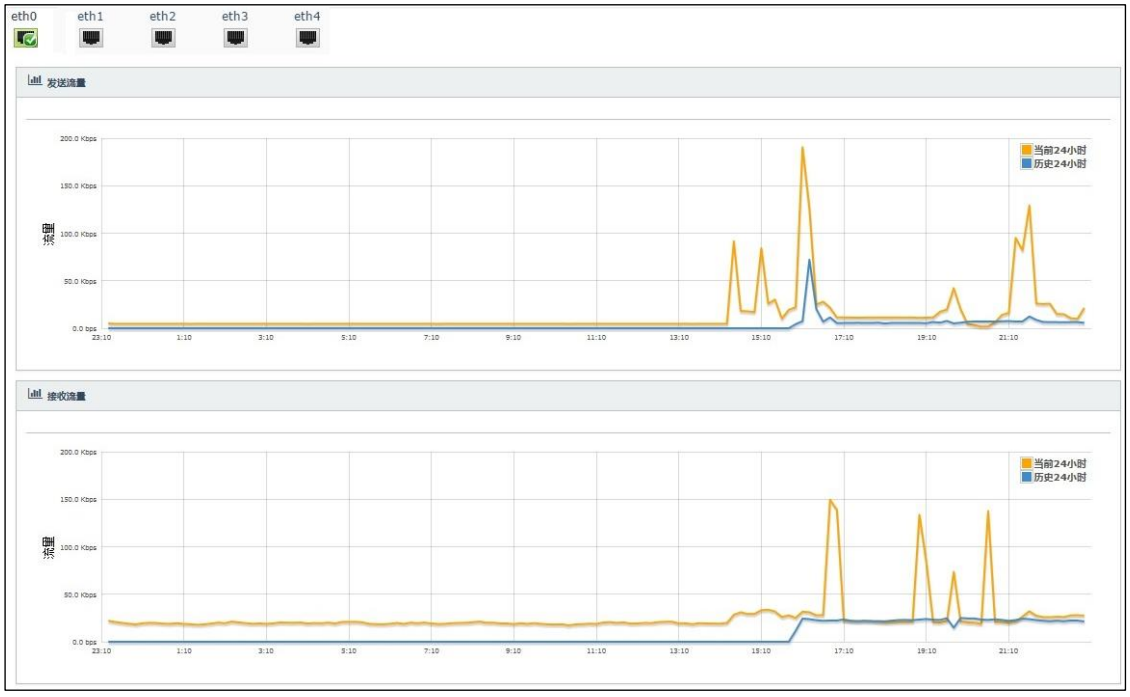
- UDP 字节数和数据包数



- ICMP 字节数和数据包数



4. 点击**历史数据流量**，可以查看接口接收和发送的历史数据流量信息。



10.4.2. 查看审计信息

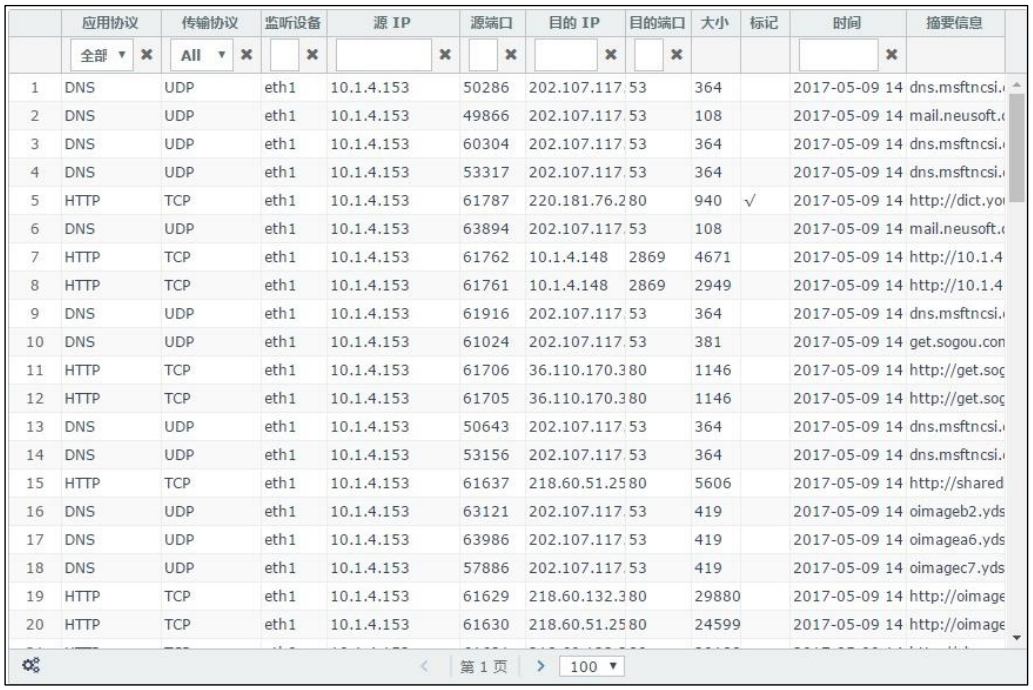
在报警配置中开启日志记录功能后，系统可记录攻击日志并用于网络审计。

要查看网络审计信息，请以安全管理员身份登录，并执行以下操作：

1. 选择**网络审计>攻击检测**，查看检测到的攻击事件。

	事件名称	事件等级	监听设备	协议	源 IP	源端口	目的 IP	目的端口	重复次数	时间	
		全部		A							
1	HP Network Node Manag		eth1	UDP	10.0.3.46	54955	10.0.3.88	7426	1	2018-11-27 15:22:29	
2	SAP-DB/MaxDB WebDBN		eth1	TCP	188.1.5.237	20438	189.1.30.24	9999	1	2018-11-27 15:22:29	
3	University of Washingtor		eth1	TCP	10.0.3.113	8301	10.0.3.125	143	1	2018-11-27 15:22:29	
4	University of Washingtor		eth1	TCP	10.0.3.113	8187	10.0.3.125	143	1	2018-11-27 15:22:29	
5	University of Washingtor		eth1	TCP	172.22.5.218	40770	172.22.5.166	143	1	2018-11-27 15:22:28	
6	Sophos病毒库Visio扫描远		eth1	TCP	10.0.3.9	14302	192.168.234.136	1177	1	2018-11-27 15:22:28	
7	Sophos病毒库Visio扫描远		eth1	TCP	10.0.3.9	46026	192.168.234.136	1114	1	2018-11-27 15:22:28	
8	Microsoft IE URLMON.DL		eth1	TCP	1.255.25.111	80	1.1.138.184	45108	2	2018-11-27 15:22:27	
9	GoodTech SMTP Server		eth1	TCP	188.1.205.13	30271	189.1.21.136	25	1	2018-11-27 15:22:27	
10	GoodTech SMTP Server		eth1	TCP	188.1.246.108	35145	189.1.227.127	25	1	2018-11-27 15:22:27	
11	Phase Zero Trojan Client		eth1	TCP	1.2.115.227	555	1.1.231.197	52712	1	2018-11-27 15:22:27	
12	Phase Zero Trojan Client		eth1	TCP	1.2.89.49	555	1.1.231.40	23035	1	2018-11-27 15:22:26	
13	网络神偷 11.1 版		eth1	UDP	10.0.0.186	3174	10.0.0.201	2018	1	2018-11-27 15:22:26	
14	Microsoft Windows即插即		eth1	TCP	1.229.96.51	2772	1.255.7.20	139	6	2018-11-27 15:22:24	
15	Microsoft Windows 2000		eth1	TCP	10.2.8.149	2564	10.2.1.60	135	4	2018-11-27 15:22:24	
16	RPC扫描		eth1	TCP	10.2.8.149	2564	10.2.1.60	135	24	2018-11-27 15:22:24	
17	Microsoft Windows 2000		eth1	TCP	10.2.8.149	2562	10.2.1.60	135	4	2018-11-27 15:22:24	
18	RPC扫描		eth1	TCP	10.2.8.149	2562	10.2.1.60	135	24	2018-11-27 15:22:23	
19	Microsoft SQL Server xp		eth1	TCP	10.2.8.149	1028	10.2.1.60	1433	8	2018-11-27 15:22:23	

2. 选择**网络审计>应用审计**，查看监听网络中的应用信息。



	应用协议	传输协议	监听设备	源 IP	源端口	目的 IP	目的端口	大小	标记	时间	摘要信息
	全部	All									
1	DNS	UDP	eth1	10.1.4.153	50286	202.107.117	53	364		2017-05-09 14	dns.msftncsi.(
2	DNS	UDP	eth1	10.1.4.153	49866	202.107.117	53	108		2017-05-09 14	mail.neusoft.(
3	DNS	UDP	eth1	10.1.4.153	60304	202.107.117	53	364		2017-05-09 14	dns.msftncsi.(
4	DNS	UDP	eth1	10.1.4.153	53317	202.107.117	53	364		2017-05-09 14	dns.msftncsi.(
5	HTTP	TCP	eth1	10.1.4.153	61787	220.181.76.2	80	940	√	2017-05-09 14	http://dict.yo(
6	DNS	UDP	eth1	10.1.4.153	63894	202.107.117	53	108		2017-05-09 14	mail.neusoft.(
7	HTTP	TCP	eth1	10.1.4.153	61762	10.1.4.148	2869	4671		2017-05-09 14	http://10.1.4
8	HTTP	TCP	eth1	10.1.4.153	61761	10.1.4.148	2869	2949		2017-05-09 14	http://10.1.4
9	DNS	UDP	eth1	10.1.4.153	61916	202.107.117	53	364		2017-05-09 14	dns.msftncsi.(
10	DNS	UDP	eth1	10.1.4.153	61024	202.107.117	53	381		2017-05-09 14	get.sogou.con
11	HTTP	TCP	eth1	10.1.4.153	61706	36.110.170.3	80	1146		2017-05-09 14	http://get.soc
12	HTTP	TCP	eth1	10.1.4.153	61705	36.110.170.3	80	1146		2017-05-09 14	http://get.soc
13	DNS	UDP	eth1	10.1.4.153	50643	202.107.117	53	364		2017-05-09 14	dns.msftncsi.(
14	DNS	UDP	eth1	10.1.4.153	53156	202.107.117	53	364		2017-05-09 14	dns.msftncsi.(
15	HTTP	TCP	eth1	10.1.4.153	61637	218.60.51.25	80	5606		2017-05-09 14	http://shared
16	DNS	UDP	eth1	10.1.4.153	63121	202.107.117	53	419		2017-05-09 14	oimageb2.yds
17	DNS	UDP	eth1	10.1.4.153	63986	202.107.117	53	419		2017-05-09 14	oimagea6.yds
18	DNS	UDP	eth1	10.1.4.153	57886	202.107.117	53	419		2017-05-09 14	oimagec7.yds
19	HTTP	TCP	eth1	10.1.4.153	61629	218.60.132.3	80	29880		2017-05-09 14	http://oimage
20	HTTP	TCP	eth1	10.1.4.153	61630	218.60.51.25	80	24599		2017-05-09 14	http://oimage

第 1 页 100

3. 选择**网络审计>连接审计**，查看监听网络中的连接信息。

传输协议	连接状态	监听设备	源 IP	目的 IP	目的端口	连接次数	请求字节数	应答字节数	时间
TCP	TCP_CLOSE	eth1	192.168.10.230	192.168.10.230	110	1	338	20407	2018-11-27 15:25:21
TCP	TCP_SYN_SENT	eth1	192.168.253.1	192.168.253.1	30000	1	0	0	2018-11-27 15:25:21
TCP	TCP_CLOSE	eth1	188.1.183.194	188.1.183.194	39069	1	5050	272	2018-11-27 15:25:21
TCP	TCP_CLOSE	eth1	188.1.217.92	188.1.217.92	49288	1	5200	272	2018-11-27 15:25:21
TCP	TCP_SYN_SENT	eth1	192.168.253.1	192.168.253.1	15001	1	0	0	2018-11-27 15:25:21
TCP	TCP_CLOSE	eth1	172.22.5.218	172.22.5.218	10051	1	128	116	2018-11-27 15:25:20
TCP	TCP_CLOSE	eth1	172.22.5.104	172.22.5.104	3306	1	42167	3186	2018-11-27 15:25:20
TCP	TCP_CLOSE	eth1	188.1.111.137	188.1.111.137	445	1	2648	1175	2018-11-27 15:25:20
TCP	TCP_CLOSE	eth1	192.168.78.132	192.168.78.132	666	1	0	142	2018-11-27 15:25:20
TCP	TCP_CLOSE	eth1	1.1.18.216	1.1.18.216	80	1	270	0	2018-11-27 15:25:19
TCP	TCP_CLOSE	eth1	192.168.1.0	192.168.1.0	30102	4	448	864	2018-11-27 15:25:19
TCP	TCP_CLOSE	eth1	192.168.1.0	192.168.1.0	30100	4	763	5368	2018-11-27 15:25:19
TCP	TCP_SYN_SENT	eth1	192.168.10.1	192.168.10.1	8080	1	0	0	2018-11-27 15:25:19
TCP	TCP_CLOSE	eth1	172.22.5.104	172.22.5.104	5900	1	52	1312	2018-11-27 15:25:18
TCP	TCP_CLOSE	eth1	172.22.5.218	172.22.5.218	7777	1	4666	82	2018-11-27 15:25:18
TCP	TCP_CLOSE	eth1	10.0.3.129	10.0.3.129	8080	1	1064	0	2018-11-27 15:25:18
TCP	TCP_CLOSE	eth1	188.1.9.138	188.1.9.138	4289	1	5143	4943	2018-11-27 15:25:17
TCP	TCP_CLOSE	eth1	188.1.9.138	188.1.9.138	1521	1	277	104	2018-11-27 15:25:17
TCP	TCP_CLOSE	eth1	1.193.253.174	1.193.253.174	1100	1	1586	0	2018-11-27 15:25:17

4. 选择**网络审计>网络信息收集**，查看监听网络中的主机信息。

	MAC地址	IP地址	主机名	组名	时间
1	021AC5FF5300	1.255.83.0			2018-11-27 13:12:12
2	0090FB48769A	10.0.3.1			2018-11-27 13:16:19
3	000FE2E114DD	192.168.122.1			2018-11-27 13:15:01
4	005056C00008	192.168.64.1			2018-11-27 13:13:34
5	005056C00008	192.168.253.1			2018-11-27 13:12:57
6	0090FB062CFA	10.0.0.1			2018-11-27 13:12:52
7	000FE2E114DD	192.168.75.1			2018-11-27 13:12:48
8	001380D59A2F	172.16.1.1			2018-11-27 13:12:36
9	005056C00001	192.168.80.1			2018-11-27 13:12:36
10	005056C00008	192.168.78.1			2018-11-27 13:12:31
11	0015179C91FC	10.0.3.1			2018-11-27 13:12:27
12	005056F229AE	192.168.58.2			2018-11-27 13:16:36
13	005056E1F25A	192.168.186.2			2018-11-27 13:16:36
14	000C29207895	10.0.24.2			2018-11-27 13:15:45
15	0090FB0D20BD	10.0.24.2			2018-11-27 13:15:18